



ID: 339451
Sample Name: sample4.bin
Cookbook: default.jbs
Time: 04:01:56
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report sample4.bin 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 4
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Compliance: 5
E-Banking Fraud: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Stealing of Sensitive Information: 5
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 13
Public 14
Private 14
General Information 14
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASN 16
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 18
Static File Info 24
General 24
File Icon 24
Static PE Info 24
General 24
Entrypoint Preview 25
Data Directories 26
Sections 26
Resources 26

Copyright null 2021

Imports 27
Version Infos 28
Possible Origin 29
Network Behavior 29
Network Port Distribution 29
TCP Packets 29
UDP Packets 31
DNS Queries 32
DNS Answers 33
HTTPS Packets 33
Code Manipulations 34
Statistics 34
Behavior 34
System Behavior 34
Analysis Process: sample4.exe PID: 2100 Parent PID: 5880 34
General 34
File Activities 34
Analysis Process: WerFault.exe PID: 1488 Parent PID: 2100 34
General 35
File Activities 35
File Created 35
File Deleted 35
File Written 35
Registry Activities 58
Key Created 58
Key Value Created 58
Analysis Process: WerFault.exe PID: 5920 Parent PID: 2100 59
General 59
File Activities 59
File Created 59
File Deleted 60
File Written 60
Registry Activities 83
Key Created 83
Analysis Process: WerFault.exe PID: 620 Parent PID: 2100 83
General 83
File Activities 84
File Created 84
File Deleted 84
File Written 84
Registry Activities 107
Key Created 107
Analysis Process: WerFault.exe PID: 5008 Parent PID: 2100 107
General 107
File Activities 108
File Created 108
File Deleted 108
File Written 108
Registry Activities 131
Key Created 131
Analysis Process: WerFault.exe PID: 5764 Parent PID: 2100 131
General 131
File Activities 132
File Created 132
File Deleted 132
File Written 132
Registry Activities 155
Key Created 155
Disassembly 155
Code Analysis 155

Copyright null 2021

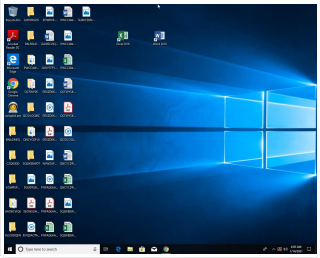
Analysis Report sample4.bin

Overview

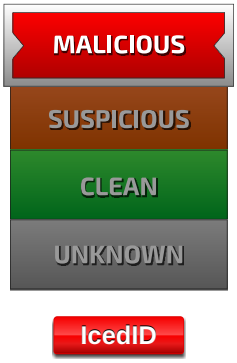
General Information

Sample Name:	sample4.bin (renamed file extension from bin to exe)
Analysis ID:	339451
MD5:	5009b8bcf024704.
SHA1:	df607367a88b561.
SHA256:	30f099660904079.

Most interesting Screenshot:



Detection

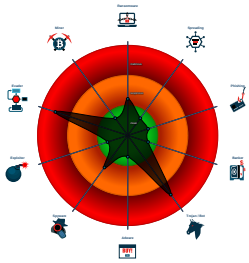


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected IcedID
- Yara detected IcedID
- Contains functionality to detect hard…
- Abnormal high CPU Usage
- Checks if the current process is bein…
- Contains functionality for execution …
- Contains functionality to check if a d…

Classification



Startup

- **System is w10x64**
- sample4.exe (PID: 2100 cmdline: 'C:\Users\user\Desktop\sample4.exe' MD5: 5009B8BCF024704C8B23E42C492F118C)
  - WerFault.exe (PID: 1488 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2100 -s 768 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5920 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2100 -s 804 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 620 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2100 -s 896 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5008 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2100 -s 924 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5764 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2100 -s 1224 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.362692606.0000000001320000.00000040.00000001.sdmp	JoeSecurity_IcedID_3	Yara detected IcedID	Joe Security	
00000000.00000002.551228989.00000000000D1000.00000020.00020000.sdmp	JoeSecurity_IcedID_3	Yara detected IcedID	Joe Security	
Process Memory Space: sample4.exe PID: 2100	JoeSecurity_IcedID_1	Yara detected IcedID	Joe Security	

Unpacked PEs

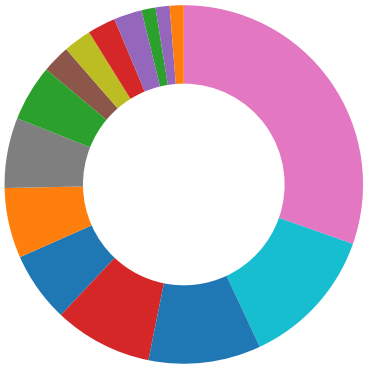
Source	Rule	Description	Author	Strings
0.2.sample4.exe.d0000.0.unpack	JoeSecurity_IcedID_3	Yara detected IcedID	Joe Security	

Copyright null 2021

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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:



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Yara detected IcedID

Yara detected IcedID

Compliance:



Detected unpacking (overwrites its own PE header)

E-Banking Fraud:



Yara detected IcedID

Yara detected IcedID

Data Obfuscation:



Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:



Contains functionality to detect hardware virtualization (CPUID execution measurement)

Stealing of Sensitive Information:



Yara detected IcedID

Yara detected IcedID

Remote Access Functionality:



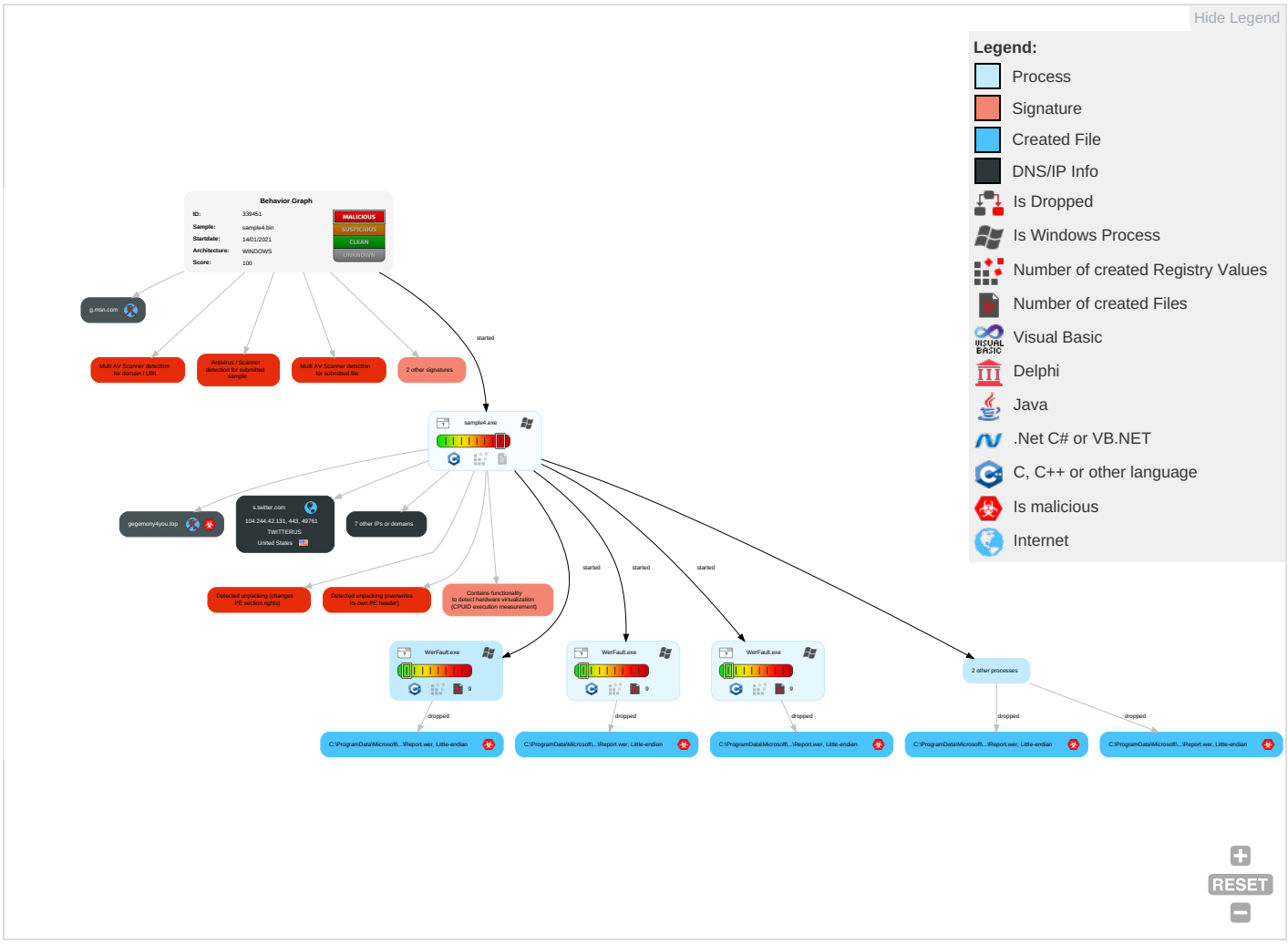
Yara detected IcedID

Yara detected IcedID

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 2	Path Interception	Process Injection 2	Virtualization/Sandbox Evasion 2	Input Capture 1 1	System Time Discovery 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Security Software Discovery 1 5 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Virtualization/Sandbox Evasion 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 2	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Owner/User Discovery 1	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	Remote System Discovery 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	File and Directory 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	System Information Discovery 1 1 3	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

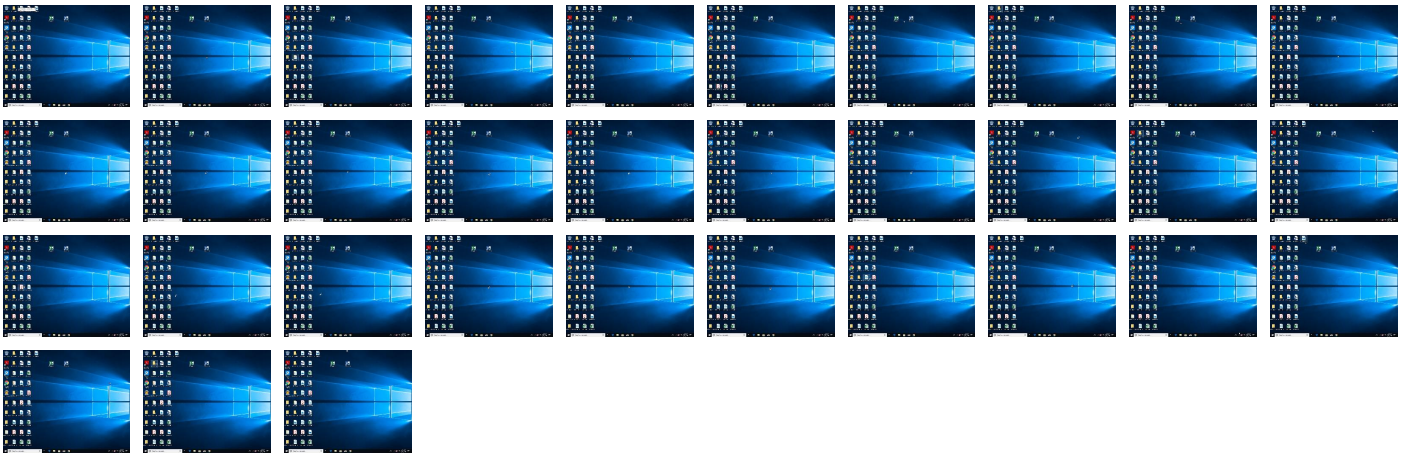
Behavior Graph



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
sample4.exe	77%	Virustotal		Browse
sample4.exe	3%	Metadefender		Browse
sample4.exe	79%	ReversingLabs	Win32.Worm.Cridex	
sample4.exe	100%	Avira	TR/IcedId.ltfzr	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.sample4.exe.d0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
gegemony4you.top	6%	Virustotal		Browse
www.intel.ch	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://static.ads-twitter.com	0%	URL Reputation	safe	
http://https://static.ads-twitter.com	0%	URL Reputation	safe	
http://https://static.ads-twitter.com	0%	URL Reputation	safe	
http://https://static.ads-twitter.com	0%	URL Reputation	safe	
http://https://cdn.cms-twdigitalassets.com/content/dam/help-twitter/logos/card_wide_blue.png	0%	Avira URL Cloud	safe	
http://https://cdn.cms-twdigitalassets.com	0%	Virustotal		Browse
http://https://cdn.cms-twdigitalassets.com	0%	Avira URL Cloud	safe	
http://https://cdn.goglobalwithtwitter.com	0%	Avira URL Cloud	safe	
http://https://feedback.digital-cloud-prem.medallia.com;	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
s.twitter.com	104.244.42.131	true	false		high
support.oracle.com	unknown	unknown	false		high
www.oracle.com	unknown	unknown	false		high
g.msn.com	unknown	unknown	false		high
help.twitter.com	unknown	unknown	false		high
www.intel.com	unknown	unknown	false		high
gegemony4you.top	unknown	unknown	true	• 6%, Virustotal, Browse	unknown
www.intel.ch	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
corpredirect.intel.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.live.com/owa/	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/using-twitter#search-and-trends	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/managing-your-account/notifications-on-mobile-devices	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/fr	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://about.twitter.com/en_us/safety.html	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://developer.twitter.com/en/docs	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/managing-your-account#login-and-password	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://blog.twitter.com/	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/fil	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high
http://https://about.twitter.com/en_us/company.html	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/nl	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532297635.000000000153E000.00000004.00000001.sdmp	false		high

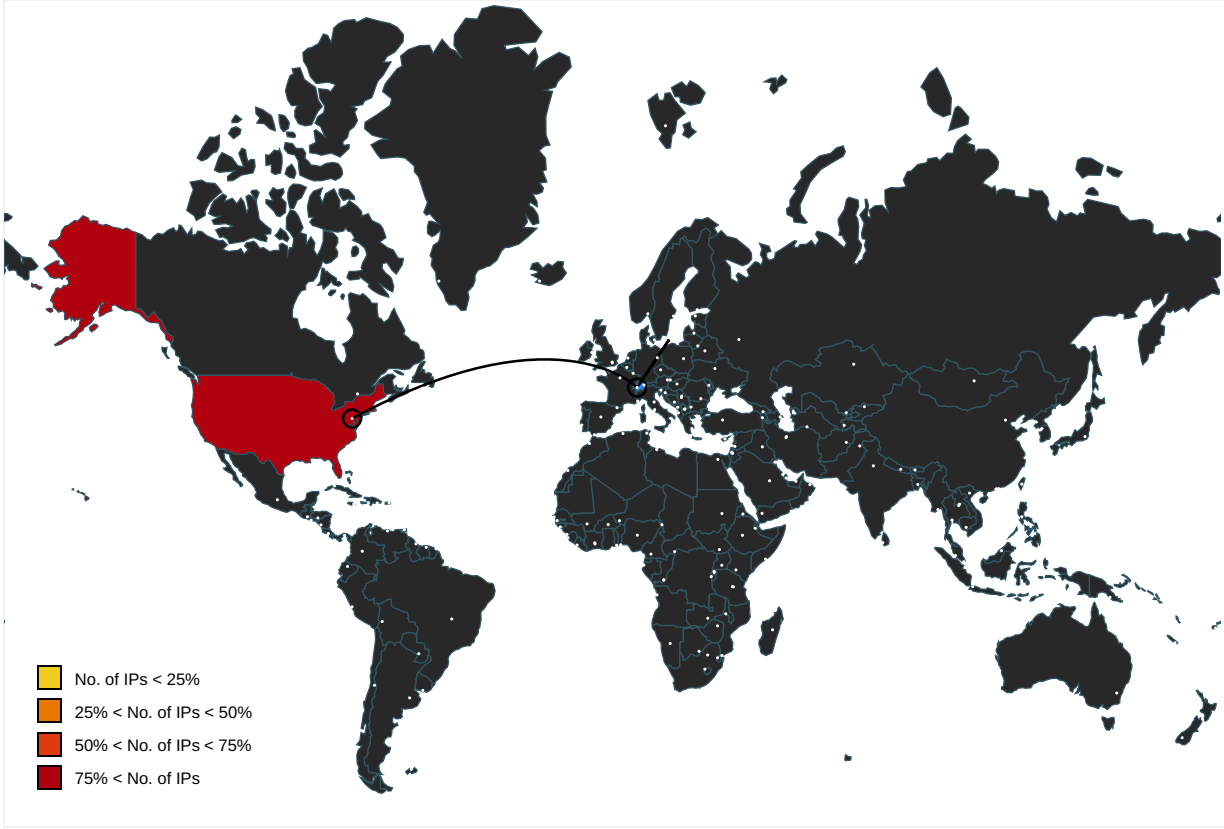
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://help.twitter.com/fa	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high
http://https://twitter.com/AppleSupport	sample4.exe, 00000000.00000003.545079805.0000000003C0D000.00000004.00000001.sdmp	false		high
http://https://twitter.com/applesupport	sample4.exe, 00000000.00000003.545079805.0000000003C0D000.00000004.00000001.sdmp	false		high
http://https://resources.digital-cloud-prem.medallia.com	sample4.exe, 00000000.00000003.533332045.0000000001539000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/fi	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high
http://https://templates.office.com/	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://twitter.com/i/csp_report;	sample4.exe, 00000000.00000003.533332045.0000000001539000.00000004.00000001.sdmp	false		high
http://https://business.twitter.com/en/advertising.html	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/no	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high
http://https://static.ads-twitter.com	sample4.exe, 00000000.00000003.533332045.0000000001539000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://help.twitter.com/en/rules-and-policies/twitter-rules	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://cdn.cms-twdigitalassets.com/content/dam/help-twitter/logos/card_wide_blue.png	sample4.exe, 00000000.00000003.532297635.000000000153E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://help.twitter.com/gu	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high
http://https://api.twitter.com	sample4.exe, 00000000.00000003.533332045.0000000001539000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/using-twitter#adding-content-to-your-tweet	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://blog.twitter.com/en_us/topics/company/2020/covid-19.html	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high
http://https://twitter.com	sample4.exe, 00000000.00000003.533332045.0000000001539000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532297635.000000000153E000.00000004.00000001.sdmp	false		high
http://https://www.twitterflightschool.com/sl/382652bc	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/rules-and-policies#law-enforcement-guildelines	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://login.microsoftonline.com/common/oauth2/authorize?response_mode=form_post	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://support.xbox.com/	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/managing-your-account	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/using-twitter/mentions-and-replies	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/rules	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.cms-twdigitalassets.com	sample4.exe, 00000000.00000003.533332045.0000000001539000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.wikidata.org/wiki/Q65129345	sample4.exe, 00000000.00000003.545079805.0000000003C0D000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/a-safer-twitter	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high
http://https://transparency.twitter.com/	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://business.twitter.com/en/help.html	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/twitter-guide	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://cdn.goglobalwithtwitter.com	sample4.exe, 00000000.00000003.533332045.0000000001539000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schema.org/VideoObject	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/using-twitter/tweeting-gifs-and-pictures	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/how-you-can-control-your-privacy	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/using-twitter/advanced-twitter-mute-options	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://careers.twitter.com/	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://support.xbox.com	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/hu	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high
http://https://blog.twitter.com/developer/	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://www.microsoftstore.com/store/msusa/en_US/DisplayAddEditPaymentPage/	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com	sample4.exe, 00000000.00000003.532297635.000000000153E000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/hr	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532297635.000000000153E000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://www.microsoftstore.com/store/msusa/en_US/wishlists?Wt.mc_id=wishlist_landingpage	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://www.microsoftstore.com/store/msusa/en_US/DisplayFindYourOrderPage/nextAction.DisplayAccountR	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://www.skype.com/en/	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/managing-your-account#verified-accounts	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://media.twitter.com/	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.microsoftstore.com/store/msusa/en_US/DisplayFindYourOrderPage/nextAction.DisplayAccountO	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/he	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high
http://https://data.twitter.com/	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://developer.twitter.com/en/community	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/pl	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high
http://https://schema.org	sample4.exe, 00000000.00000003.545079805.0000000003C0D000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/managing-your-account#notifications	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://status.twitterstat.us/	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/pt	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/hi	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532297635.000000000153E000.00000004.00000001.sdmp	false		high
http://https://www.onenote.com/	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/rules-and-policies#twitter-rules	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/it	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532297635.000000000153E000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/glossary	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/ja	sample4.exe, 00000000.00000003.532297635.000000000153E000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://cards-dev.twitter.com/validator	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://ogp.me/ns#	sample4.exe, 00000000.00000003.532297635.000000000153E000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/ar	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532297635.000000000153E000.00000004.00000001.sdmp	false		high
http://https://about.twitter.com/en_us/company/twitter-for-good.html	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://privacy.twitter.com/	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/using-twitter#tweets	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://marketing.twitter.com/en/insights	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://about.twitter.com/en_us/company/brand-resources.html	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/id	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532297635.000000000153E000.00000004.00000001.sdmp	false		high
http://schema.org/Organization	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://twitter.com/login?redirect_after_login=https://help.twitter.com/en	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high
http://https://business.twitter.com/en/resources.html	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/contact-us	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://video.twimg.com/tweet_video/EAa_YvRU4AAH-IN.mp4	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://business.twitter.com/	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/bn	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://feedback.digital-cloud-prem.medallia.com;	sample4.exe, 00000000.00000003.533332045.0000000001539000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://twitter.com/privacy	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/sk	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp, sample4.exe, 00000000.00000003.532297635.000000000153E000.00000004.00000001.sdmp	false		high
http://https://templates.office.com/collection-family-activities	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://www.microsoftstore.com/store/msusa/en_US/DisplayFindYourOrderPage/nextAction.DisplayDownload	sample4.exe, 00000000.00000003.519277199.000000000152B000.00000004.00000001.sdmp	false		high
http://https://marketing.twitter.com/en/success-stories	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://twitter.com/logout	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/en/using-twitter/direct-messages	sample4.exe, 00000000.00000003.532203579.0000000003C01000.00000004.00000001.sdmp	false		high
http://https://help.twitter.com/ro	sample4.exe, 00000000.00000003.532275265.0000000001546000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.244.42.131	unknown	United States		13414	TWITTERUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339451
Start date:	14.01.2021
Start time:	04:01:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sample4.bin (renamed file extension from bin to 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
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

Copyright null 2021

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/20@8/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.6% (good quality ratio 1.5%) • Quality average: 78.6% • Quality standard deviation: 26.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, RuntimeBroker.exe, wermgr.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 52.147.198.201, 2.20.84.85, 20.190.129.19, 40.126.1.142, 20.190.129.2, 40.126.1.130, 40.126.1.145, 20.190.129.128, 20.190.129.160, 20.190.129.130, 51.11.168.160, 93.184.221.240, 92.122.213.194, 92.122.213.247, 20.54.26.129, 104.43.139.144, 51.104.139.180, 52.142.114.176, 40.88.32.150, 104.83.125.175, 104.83.83.83, 2.20.84.4, 2.21.61.56, 2.20.84.208, 2.17.181.200, 52.155.217.156 • Excluded domains from analysis (whitelisted): intel11.edgekey.net, arc.msn.com.nsatc.net, intel11.cn.edgekey.net, support-china.apple-support.akadns.net, fs-wildcard.microsoft.com.edgekey.net, ev.support.microsoft.com.edgekey.net, skypedataprdcoleus15.cloudapp.net, prod-support.apple-support.akadns.net, support.oracle.com.edgekey.net, e3843.g.akamaiedge.net, login.live.com, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, fs.microsoft.com, e2581.dscx.akamaiedge.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, www.tm.a.prd.aadg.akadns.net, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, e2063.e9.akamaiedge.net, e11.dsca.akamaiedge.net, blobcollector.events.data.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.net, intel19233.edgekey.net, e19233.dsca.akamaiedge.net, support.microsoft.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, intel11.cn.edgekey.net.globalredir.akadns.net, support.apple.com, support.apple.com.edgekey.net, cs11.wpc.v0cdn.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, e870.x.akamaiedge.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, wu.ec.azureedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ds-www.oracle.com.edgekey.net, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:04:49	API Interceptor	9x Sleep call for process: sample4.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.244.42.131	http://https://cypressbayhockey.com/NO	Get hash	malicious	Browse	
	details.html	Get hash	malicious	Browse	
	details.html	Get hash	malicious	Browse	
	http://https://numisconsult.com/blog/e47c4b8720db7445599988579a03c7c5	Get hash	malicious	Browse	
	http://https://sosefinawinnifredsullivan8-5ce0e.gr8.com/	Get hash	malicious	Browse	
	http://kikicustomwigs.com/inefficient.php	Get hash	malicious	Browse	
	http://https://www.evernote.com/shard/s395/sh/e6cd3f32-356e-2b0f-29eb-532205cb0cdd/b301c5a7d8494fe2a6f2588862012fb5	Get hash	malicious	Browse	
	http://https://doc.clickup.com/p/h/853bx-28/ee9d693560ec8e5	Get hash	malicious	Browse	
	http://https://doc.clickup.com/p/h/84zph-7/c3996c24fc61b45	Get hash	malicious	Browse	
	http://https://cts.indeed.com/v0?tk=1df9t5skc2g3980p&r=%68%74%74%70%73%3a%2f%2f%61%6e%61%6c%79%74%69%63%73%2e%74%77%69%74%74%65%72%2e%63%6f%6d%2f%64%61%61%2f%30%2f%64%61%61%5f%6f%70%74%6f%75%74%5f%61%63%74%69%6f%6e%73%3f%61%63%74%69%6f%6e%5f%69%64%3d%33%26%70%61%72%74%69%63%69%70%61%6e%74%5f%69%64%3d%37%31%36%26%72%64%3d%68%74%74%70%73%3a%2f%2f%66%72%61%31%2e%64%69%67%69%74%61%6c%6f%63%65%61%6e%73%70%61%63%65%73%2e%63%6f%6d%2f%73%32%32%2f%69%6e%64%65%78%2e%68%74%6d%6c%3f#matthias.kirsch@iti.org	Get hash	malicious	Browse	
	WSGaRIW.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Mikey.116711.25037.dll	Get hash	malicious	Browse	
	http://https://call.lifesizecloud.com/4478671	Get hash	malicious	Browse	
	VSMecyU.dll	Get hash	malicious	Browse	
	http://https://recovermy3-account.com/	Get hash	malicious	Browse	
	http://https://recovermy3-account.com/	Get hash	malicious	Browse	
	temp.dll	Get hash	malicious	Browse	
	iuyala11.dll	Get hash	malicious	Browse	
	temp.dll	Get hash	malicious	Browse	
	temp.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
s.twitter.com	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 104.244.42.131
	http://search.hshipmenttracker.co	Get hash	malicious	Browse	• 104.244.42.67
	http://https://t.yesware.com/tt/ae9851ab7b578dad1289f08bbf450624f7ae3a45/2ee42987f58d2f32bb36ff11a00dd921/2f4e7e35c28c3b7f4958904f5584a915/joom.ag/2VFC	Get hash	malicious	Browse	• 104.244.42.195
	http://https://joom.ag/3wFC	Get hash	malicious	Browse	• 104.244.42.3

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TWITTERUS	http://message.mydopweb.com	Get hash	malicious	Browse	• 104.244.42.193
	http://www.secured-mailsharepoint.online/	Get hash	malicious	Browse	• 104.244.42.130

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.ensonoelevate2021.com/event/8e8c2672-3b18-40b1-8efc-026ab72e6424/summary?environment=P2&5S%2CM3%2C8e8c2672-3b18-40b1-8efc-026ab72e6424=	Get hash	malicious	Browse	• 104.244.42.5
	http://https://cypressbayhockey.com/NO	Get hash	malicious	Browse	• 104.244.42.197
	details.html	Get hash	malicious	Browse	• 104.244.42.5
	details.html	Get hash	malicious	Browse	• 104.244.42.5
	http://https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/?utm_source=redcanary&utm_medium=email&utm_campaign=Blog%20Digest-2020-11-05T09:00:54.888-07:00&mkt_tok=eyJpIjoiWmpKbVlUTXpPRGMzTTJRMSIsInQiOiJtMm9iYWJESHd5VldFUTF2a05zeEdtVUdMNms3cHVcL01OcW9hYUlwOElYZFwvNkdvd0UzV0x2SDdNZVlIMWFTSG1jS28zM0JIamh3YXRvcmU0K2htaTJpTlFLbjNNaWswT2NxYlhXdElEZHVzMlFaclpoTUFzZk1ibTV0SGVwSCs2In0%3D	Get hash	malicious	Browse	• 104.244.42.133
	http://https://patrickphimr5.github.io/memoaideivozx/dsfriet.html?bbre=dxcfdgoiss	Get hash	malicious	Browse	• 104.244.42.65
	http://https://doc.clickup.com/p/h/2hm67-99/806f7673f7694a9	Get hash	malicious	Browse	• 104.244.42.3
	http://aypf.z2systems.com	Get hash	malicious	Browse	• 104.244.42.193
	http://https://create.piktochart.com/output/51658503-cfo-capabel	Get hash	malicious	Browse	• 104.244.42.2
	http://https://protect-us.mimecast.com/s/JFIWCVON1NCzq3ggtGInaq	Get hash	malicious	Browse	• 104.244.42.67
	http://g1security.co.tz	Get hash	malicious	Browse	• 104.244.42.129
	http://https://numisconsult.com/blog/e47c4b8720db7445599988579a03c7c5	Get hash	malicious	Browse	• 104.244.42.131
	http://search.hshipmenttracker.co	Get hash	malicious	Browse	• 104.244.42.197
	http://https://sosefinawinnifredsullivan8-5ce0e.gr8.com/	Get hash	malicious	Browse	• 104.244.42.131
	http://https://t.co/2QNQz4sNnh?amp=1	Get hash	malicious	Browse	• 104.244.42.69
	http://https://omsd-org.gq/?login=do&c=E,1,MTY2COfqGo5C-H4KALYqrUyXXPpd2evSCW3stb24PsdKe8xYdoYVhcjchdnzpUCr95AnX7X4QDVSQFpJtN_EpMZ8u2smwVQNUpYGz7Etn-l-NVb_st2_649iVg,,&typo=1	Get hash	malicious	Browse	• 104.244.42.197
	http://www.cqdx.ru	Get hash	malicious	Browse	• 104.244.42.193
	http://kikicustomwigs.com/inefficient.php	Get hash	malicious	Browse	• 104.244.42.5

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	WFLPGBTMZH.dll	Get hash	malicious	Browse	• 104.244.42.131
	Customer_Receivables_Aging_20210112_2663535345242424242.exe	Get hash	malicious	Browse	• 104.244.42.131
	Listings.exe	Get hash	malicious	Browse	• 104.244.42.131
	Transferencia,pdf.exe	Get hash	malicious	Browse	• 104.244.42.131
	Dhl Client Invoice.exe	Get hash	malicious	Browse	• 104.244.42.131
	64D5aP6jQz.exe	Get hash	malicious	Browse	• 104.244.42.131
	mscthef-Fichero-ES.msi	Get hash	malicious	Browse	• 104.244.42.131
	New inquiry CON 20-10630.exe	Get hash	malicious	Browse	• 104.244.42.131
	RLFGB8pdA6.exe	Get hash	malicious	Browse	• 104.244.42.131
	ORDER#9403.exe	Get hash	malicious	Browse	• 104.244.42.131
	CLIDSXX.exe	Get hash	malicious	Browse	• 104.244.42.131
	SecuriteInfo.com.Variant.Graftor.893032.186.exe	Get hash	malicious	Browse	• 104.244.42.131
	ptrb-ES-2999223.msi	Get hash	malicious	Browse	• 104.244.42.131
	T9tAui44l4.exe	Get hash	malicious	Browse	• 104.244.42.131
	E8Jkw96qFU.exe	Get hash	malicious	Browse	• 104.244.42.131
	SecuriteInfo.com.Trojan.DownLoader36.32796.17922.exe	Get hash	malicious	Browse	• 104.244.42.131
	y46XVvLaVc.exe	Get hash	malicious	Browse	• 104.244.42.131
	Softerra Adaxes 2011.3.exe	Get hash	malicious	Browse	• 104.244.42.131
	r0u.exe	Get hash	malicious	Browse	• 104.244.42.131
	r0u.exe	Get hash	malicious	Browse	• 104.244.42.131

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_023208c1\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12180
Entropy (8bit):	3.7757129548768527
Encrypted:	false
SSDEEP:	96:4nnLHJPBHQToA7Rb6tpXIQcQnc6rCcEhcw3r7+HbHg/PtuuzOOFLMbsWoxMfpNq9:gDJP/H56rQjzEfKXR/u7sxS274Itxpq
MD5:	F33A74C78B60DE4948ABD5FCA62C8C1D
SHA1:	6DAAA0FBCDF61CA7594A921A457A0CB428B16CD0
SHA-256:	7514782350B6350389B11D177F2F9CB6CABB95F4AEC9E8377EA9248A1722710B
SHA-512:	25E287B740FC747C4646DBC5CF1E80EE6384608864AD305711DAC723D099BCF78A4F2ADD7D4AEB6B1D99D01E3EA215275D2D75922885F171A827180B2F3E525
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.5.0.9.9.4.6.1.3.3.4.6.1.7.1.....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.=.6.f.5.0.1.7.1.e.-.c.7.a.3.-.4.6.b.a.-.b.c.8.5.-.2.2.a.8.f.7.6.b.b.f.2.8.....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.=.a.0.1.7.c.2.6.2.-.0.1.5.3.-.4.5.2.c.-.b.7.6.6.-.5.8.7.5.9.a.0.7.8.d.5.e.....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.a.m.p.l.e.4...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.a.r.r.a...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.8.3.4.-.0.0.0.1.-.0.0.1.7.-.c.7.f.b.-.d.e.2.b.6.d.e.a.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.8.a.f.e.e.8.1.a.7.5.1.5.4.c.b.b.d.8.a.0.f.f.7.c.2.f.6.3.6.9.d.0.0.0.0.0.9.0.4.!.0.0.0.0.d.f.6.0.7.3.6.7.a.8.8.b.5.6.1.0.a.2.2.4.9.0.9.e.f.b.8.d.e.b.e.b.0.d.9.0.f.4.8.7.!.s.a.m.p.l.e.4...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.0.4././.0.7.:.1.0.:.4.4.:.1.6.!.0.!.s.a.m.p.l.e.4...

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_058db978\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12080
Entropy (8bit):	3.7723760710787007
Encrypted:	false
SSDEEP:	96:YOIarJPFHQToA7Rb6tpXIQcQnc6rCcEhcw3r7+HbHg/PtuuzOOFLMbsWoxMfpNqy:6EJPbH56rQjzEfKXR/u7sWS274Itxp6
MD5:	8549CFB0ABB89E6BA07A896B3BAEB4FF
SHA1:	47BE65FFBEFFAB2884B681F321D4E329A339F28F
SHA-256:	36614A01566DE26BCAEC36177422C484B9ED2A5FAA8061A7D528680323D0346C
SHA-512:	B7B09418ACBE27182027B3FBAE153444AF2CB6FC5F39002D59546B583A4948A660FDC9F75D1802429071539830D0E4794E0473B06BD910DBAC300E72C67124A5
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.5.0.9.9.4.4.2.2.4.0.9.1.7.5.....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.e.c.a.1.6.6.0.-.2.6.1.0.-.4.1.e.8.-.b.8.4.2.-.5.0.d.3.e.2.3.6.3.a.f.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.=.d.0.d.0.d.3.9.4.-.c.d.b.f.-.4.d.a.6.-.b.2.d.9.-.0.e.5.c.4.d.d.5.2.e.4.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.a.m.p.l.e.4...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.a.r.r.a...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.8.3.4.-.0.0.0.1.-.0.0.1.7.-.c.7.f.b.-.d.e.2.b.6.d.e.a.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.8.a.f.e.e.8.1.a.7.5.1.5.4.c.b.b.d.8.a.0.f.f.7.c.2.f.6.3.6.9.d.0.0.0.0.0.9.0.4.!.0.0.0.0.d.f.6.0.7.3.6.7.a.8.8.b.5.6.1.0.a.2.2.4.9.0.9.e.f.b.8.d.e.b.e.b.0.d.9.0.f.4.8.7.!.s.a.m.p.l.e.4...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.0.4././.0.7.:.1.0.:.4.4.:.1.6.!.0.!.s.a.m.p.l.e.4...

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_13ce361a\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12384
Entropy (8bit):	3.775237108429829
Encrypted:	false
SSDEEP:	96:g9HQJPrHQToA7Rb6tpXIQcQnc6rCcEhcw3r7+HbHg/PtuuzOOFLMbsWoxMfpNqEY:PJP1H56rQjzEfKX0/u7sxS274Itxpv
MD5:	A83850FBB51EE9A273A439B5D0CEE57E
SHA1:	379A2AA130BF3AA164B9FF6C1E09508E4C21D122
SHA-256:	A66236E86CF2B98ABAC970EF37589CB14E684DF8AAF6928EF58D4C563EBB4F7E
SHA-512:	DA8583D262A7139EC32D20E9CDBAE2FC5F0A948F4889CCA9467286B5F5AABBF2E801D823767A3EF7F146AA4C62947842030DD25533F898DEFA163A1555E192E
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.5.0.9.9.4.7.4.1.4.7.0.9.2.8.....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.8.5.b.1.3.a.7.-.1.0.3.c.-.4.c.5.a.-.b.b.3.5.-.8.e.e.d.6.5.6.7.8.1.c.3.....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.=.2.2.b.e.6.5.1.e.-.8.5.e.0.-.4.6.1.5.-.9.f.4.6.-.c.f.9.8.4.8.6.2.c.5.8.b.....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.a.m.p.l.e.4...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.a.r.r.a...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.8.3.4.-.0.0.0.1.-.0.0.1.7.-.c.7.f.b.-.d.e.2.b.6.d.e.a.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.8.a.f.e.e.8.1.a.7.5.1.5.4.c.b.b.d.8.a.0.f.f.7.c.2.f.6.3.6.9.d.0.0.0.0.0.9.0.4.!.0.0.0.0.d.f.6.0.7.3.6.7.a.8.8.b.5.6.1.0.a.2.2.4.9.0.9.e.f.b.8.d.e.b.e.b.0.d.9.0.f.4.8.7.!.s.a.m.p.l.e.4...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.0.4././.0.7.:.1.0.:.4.4.:.1.6.!.0.!.s.a.m.p.l.e.4...

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_16da5cdc\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13300
Entropy (8bit):	3.7692678717959778
Encrypted:	false
SSDEEP:	96:1q5DJPmHQToA7Rb6tpXIQcQnc6rCcEhcw3r7+HbHg/PtuuzOOFLMbsWoxMfpNqEg:iJPAH56rQjzEfKX1r/u7sxS274Itxpo
MD5:	39D1F56E6FF74B3E803A3DB436DC0567
SHA1:	D353F7D0519C76D8CA38ADA8DF241FC8186AF0F8
SHA-256:	ED3D8B5ED2B208991F4041604523D134C2939875FEB9DD22DA31FC5956FECF3C
SHA-512:	C7395B8FA4F20D0EA4BB8A686AE625BE3352EC6A42AF74A0DBD9AA0E475D2009B5CEE2AE9D725C989D4C16B58390C02F4AC4FD11D39972A2CB683A6F0B5162 26
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.5.0.9.9.4.8.2.6.1.5.8.5.1.3.....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.=.0.f.6.8.4.b.1.f.-.b.5.a.a.-.4.0.5.d.-.a.c.b.b.-.8.a.d.9.c.6.c.4.f.1.e.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.=.a.d.c.4.b.4.d.0.-.2.5.0.d.-.4.4.b.5.-.a.8.4.3.-.0.e.5.9.1.7.e.2.2.0.1.2.....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.a.m.p.l.e.4...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.a.r.r.a...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.8.3.4.-.0.0.0.1.-.0.0.1.7.-.c.7.f.b.-.d.e.2.b.6.d.e.a.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.8.a.f.e.e.8.1.a.7.5.1.5.4.c.b.b.d.8.a.0.f.f.7.c.2.f.6.3.6.9.d.0.0.0.0.0.9.0.4.!.0.0.0.0.d.f.6.0.7.3.6.7.a.8.8.b.5.6.1.0.a.2.2.4.9.0.9.e.f.b.8.d.e.b.e.b.0.d.9.0.f.4.8.7.!.s.a.m.p.l.e.4...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.0.4././.0.7.:.1.0.:.4.4.:.1.6.!.0.!.s.a.m.p.l.e.4...

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_177de25c\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12082
Entropy (8bit):	3.773622159663461
Encrypted:	false
SSDEEP:	96:SzwJPCHQToA7Rb6tpXIQcQnc6rCcEhcw3r7+HbHg/PtuuzOOFLMbsWoxMfpNqE6T:uwJPEH56rQjzEfKXR/u7sWS274ItxpX
MD5:	F9DE8B024B8D805B8F53277DADEC61E5
SHA1:	EC6E575FD9A307A7263744CCE43F6050E08FFC83
SHA-256:	8F9EF602CEB6BBA4CDA441F993EFA97E087D84DADFB4D4D183E7FD0EC7B36E03
SHA-512:	05322EF2B9BFB4BC0F26FC17E255EEC6968D2AC59114E3AC08D63C7F8B516A7C7FCB32276F98136AB81B1ECF963FBA0EB97511802471E5235A6FAB03D8C7B80 B
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.5.0.9.9.4.5.0.3.5.0.2.7.1.7.....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.=.7.b.7.7.e.e.3.6.-.e.0.4.0.-.4.5.a.f.-.b.0.c.f.-.4.2.f.5.3.c.d.1.3.3.1.6.....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.c.0.4.a.b.e.3.-.2.f.2.f.-.4.9.a.d.-.9.f.c.7.-.f.1.1.1.3.f.f.f.c.4.f.e.....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.a.m.p.l.e.4...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.a.r.r.a...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.8.3.4.-.0.0.0.1.-.0.0.1.7.-.c.7.f.b.-.d.e.2.b.6.d.e.a.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.8.a.f.e.e.8.1.a.7.5.1.5.4.c.b.b.d.8.a.0.f.f.7.c.2.f.6.3.6.9.d.0.0.0.0.0.9.0.4.!.0.0.0.0.d.f.6.0.7.3.6.7.a.8.8.b.5.6.1.0.a.2.2.4.9.0.9.e.f.b.8.d.e.b.e.b.0.d.9.0.f.4.8.7.!.s.a.m.p.l.e.4...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.0.4././.0.7.:.1.0.:.4.4.:.1.6.!.0.!.s.a.m.p.l.e.4...

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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):	8400
Entropy (8bit):	3.6980603355241612
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNioq6l8J/6YSaSUGRPgmfGuSrCpBT89bGnqsfDxim:RrlsNit6l8R6YfSUGRPgmfGuSVGnJfp
MD5:	C5C4C37BAB140B7F7183F1EA1184CD0A
SHA1:	7E389311A6D7518BA8CE1D6FD27809934EA42140
SHA-256:	67AEC99C834D15887E74691AB6993FB14CBADD5A0482E332D3AA2B8FC331F759
SHA-512:	E2E7406119D4E6E7BDB497DC60BA97DA8F19BB1A85CD704EB7437788E98BD5F06C62FB06924387C1E74C32D9016263D10E87DDFCDDE16B1728B6CF2401D9D9 F
Malicious:	false
Reputation:	low
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.>.2.1.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Jan 14 12:04:35 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	88980
Entropy (8bit):	2.000024614163454
Encrypted:	false
SSDEEP:	384:g7RA21BGylxzoEalrrZwyJPsVN1eIs6pkf7D13xqhaK7AT:glA2rGyXoEalrzPsP1eL9N40lT
MD5:	8CBBD4DF28ED24D275A5B99871F0AEE4
SHA1:	AC7743902178B19F482DF54F4D191E7EA41F41D5
SHA-256:	98E94389C6B85400A3F28EE1252AFEF8B3864112FF1B729541518A55D9D07601
SHA-512:	15935D5F2E9B3D88D74509ECEB017A12488C4ED823A8A010F0C0E801511340D02D9D86605DA13226C1342685C447BBE083BC348C10C5C3686BC210DFF5AF8E5
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....S3.`.....U.....B..... .....GenuineIntelW.....T.....4....2.`:.....0.....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\WER306E.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):	8400
Entropy (8bit):	3.6977100771396483
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNioP6IL76YSVSUr6gmfGuSrCpB889bFnqsfx3m:RrlsNiA6IL76YASUr6gmfGuSoFnJfM
MD5:	7BD3D3799E7832DB6E8F790D218F6198
SHA1:	DA33CD235E2F88038F7299C0D9A486547489823E
SHA-256:	E9740B916909FDF73EB25F1E70223088E17E80E6771BA1E586644542677406CB
SHA-512:	1B3C4D5DAE7287EF8A5E974D7FDE9D2CFAC70822F8E6A1CE1D80BF5E1E5288182EA325EA4C4716A8C52BD00198FE181D756CE4B86CB70E03C12E007913F77D D8
Malicious:	false
Reputation:	low
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.>.2.1.0.0.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER32EF.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4753
Entropy (8bit):	4.464512402648456
Encrypted:	false
SSDEEP:	48:cvIwSD8zskJgtWI97TWSC8Bd8fm8M4Jv6MFfAv+q8vc6ILJsGX7vXw3d:uITfigiSN8JSRvKPILJsGX7vXgd
MD5:	E826EDFB38864830ABE3759CDA64D964
SHA1:	E873E42E77CA0B011BF44A2616A814A94D78DD7D
SHA-256:	133CE84E255AE1177A340F2B6DCFEEEA66034B0DDAC5A6F12C9E968B4640EBBE
SHA-512:	9E95458200E71C52FEA724DD4A63A1FC5E17F556915044A22D833EACA03BC98BF4121F74F9BC3E0D6EF56D4512D0AEF7C629F0AD16682AAE75501F59AC890AD 5
Malicious:	false
Reputation:	low
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="816315" />.. <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\WER4983.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Jan 14 12:04:45 2021, 0x1205a4 type
Category:	dropped

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	
Size (bytes):	99634
Entropy (8bit):	1.9828576437490704
Encrypted:	false
SSDEEP:	384:DC3W2Ak9bpkazfErHylxzhIkv8lW0U3DSfeDZg1zH1IdYkyNXN9o+s0FHDP:DC3zAksasyXKkv8l96stjP
MD5:	B8D1A8E6D6C7382D9ED80DCE25C42A2F
SHA1:	D3872274171A35FE546DAE4A9ED22ACD9CFA59C2
SHA-256:	84214734DFEF4106844A48D535B124FE377C0D2F61C26DDE221FD9204DFF9EBA
SHA-512:	1515168F4EEF03BF1D87C022D90D54A2AB18A823E4E140CF1F51F9F1275DB7691D7DA5A6F4988F1390E1768554DDFDE6F167C9C5CC460375508C532A3ADE1E5
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....]3.`.....U.....B.....$.....GenuineIntelW.....T.....4....2.`:.....0.....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\WER4DB.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4753
Entropy (8bit):	4.463092547999117
Encrypted:	false
SSDEEP:	48:cvIwSD8zskJgtWI97TWSC8BM8fm8M4Jv6MF1+q8vc6ILJsGX7vXw3d:uITfigiSNrJSoKPILJsGX7vXgd
MD5:	E26E9D255F88D992E78511EDEA3FADF9
SHA1:	945EC689B90356703A4E19ECEBD57CA20262D43B
SHA-256:	CAE1AAC0E291E4AF14844FD194E2799CD81C7FFB27F3EB1050E1027519B60483
SHA-512:	22ED4E71392445AB7C3B9BEC66AA07A918270921199814676E984D9E96A79B7450D26B4894F4C1F8F5D3FC65D77E28C27524ACB82191BDCA20B514F0CD9E024
Malicious:	false
Reputation:	low
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="816315" />.. <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\WER55D8.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):	8402
Entropy (8bit):	3.6978315130490094
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNioR6oW6YSpSU/RUgmfGuSrCpB689bSnqsfXGm:RrlsNiO6Z6YcSU/RUgmfGuSySnJff
MD5:	DB68D6E459836A75F1E0AF2DC6BAA85A
SHA1:	2CE8D49935A1B4FDCC481D03799836985BFCC0D9
SHA-256:	3CB838BDC9B4E336895C5973F459D35E405FEF9677F8D82200E5A92A3A68527E
SHA-512:	40F4D08F3E5531C2F636A079739673811A8E5020B5F9E73BF1222C9CCBB0DCF88B03E3BD2BF3F44E47D5D1631D10A20BE99F8CCCA64F0928CB25D1C92619E4D
Malicious:	false
Reputation:	low
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.>.2.1.0.0.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER585A.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4753
Entropy (8bit):	4.461932434666514
Encrypted:	false
SSDEEP:	48:cvIwSD8zskJgtWI97TWSC8Bis8fm8M4Jv6MF5O+q8vc6ILJsGX7vXw3d:uITfigiSN8JSVKPILJsGX7vXgd

C:\ProgramData\Microsoft\Windows\WER\Temp\WER585A.tmp.xml	
MD5:	A46FB23426B471BA03A31FDE8720D575
SHA1:	CED3DAA8CC74407B7A14EC4D6EF6C1BC349E9EB9
SHA-256:	7C28650FC1F5DEC46F21CB7B42172FBB7861CF305A9F46FF2E91CEB20F2D13BD
SHA-512:	42F8F054A5A32C667D48CABA88115A6C606F988B4910B8D9F9A5BF62996F13E3BE725A108FBE6982066577800FE559D185BC1FD2A4206B347698EA28ADF0539A
Malicious:	false
Reputation:	low
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="816315" />.. <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\WERABCC.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Jan 14 12:04:04 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	60446
Entropy (8bit):	1.9975649594048102
Encrypted:	false
SSDEEP:	192:E2XIa05AgbT3ylxzcBYxZrrab1v2cDuK8Sbq8tHYzTBljqcKyF9:1Ia05AozylxzOY3rWhph8qXEBIA
MD5:	3EDA680C46EC45A8E65D4DB4AC767333
SHA1:	CFF6ECFF168973FFD267A1649458A2F88B9B318B
SHA-256:	1D4A384AC3803A0FB281104685A46862C6E74409B70F261C7854878FC0143EEF
SHA-512:	0D96C97B790B83ABC1D5D1F7CF53DBFCDC41BE82CA8C713493B9593DB3C2E04800615E94E2C7F28E605E40C0DC0A33741C50CACFDF8FA32013629C07C8112A3
Malicious:	false
Preview:	MDMP..... .....43.`.....U.....B.....GenuineIntelW.....T.....4....2.`:.....0.....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\WERB3DB.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):	8398
Entropy (8bit):	3.6958613853599918
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNioB6Iyi6YSKSU1ygmfGuSrCpB089bknqsfPjMm:RrlsNim6Iyi6YPSU1ygmfGuSgknJf1
MD5:	BC396DA9A4C55BE808F8957D45A75BDA
SHA1:	B82FC5184F1FD8A6CCE6CE4D30801360CBE22ABF
SHA-256:	4C4A11CB625991638B1C94AC99108B026D5E52D225C36346E5036387BAD450B7
SHA-512:	DEBD0015E401E880E7867A27C8E87AF98C7AD4481F9C241891AD382E1EABD7632B750D84172DBB0F47BF4A768568F57B6EDA1D89CCF983B463620B67165DD1E4
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.>.2.1.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB592.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4753
Entropy (8bit):	4.4599661127230705
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtWI97TWSC8BE8fm8M4Jv6MFw+q8vc6ILJsGX7vXw3d:uITflgiSNzJSFKPILJsGX7vXgd
MD5:	567A6E034EA0B483BEB8BB0082030E96
SHA1:	F5E2FEE7B5D5899E3F4AB1DAF398EDE53A4F9C5F
SHA-256:	BF95A9735FD0ADDB4B23F80125BB7BEF1CC56E24C46367B091E4595DC9876EB4
SHA-512:	DD4C4B57EB09F498A818D5A683059A0EB5091C4CE847FF058BFDCE73A06AC69E50B5B2BD046E0CA6882F6B5D659248AC92F716F969331B17CA78DB03FB0BEBE

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB592.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="816314" />.. <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\WERCB79.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Jan 14 12:04:12 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	87540
Entropy (8bit):	2.19600592359827
Encrypted:	false
SSDEEP:	384:ttutAzBwX8tErhMA1RUxbYc23OXylxzQzRCRnchtChjbcxIEDwnmI:HMAzBw4AeA3Ux323OXyXQzRCdKtiiDwX
MD5:	8C583E227B6B85DEEBE5B786648E2137
SHA1:	B580344D35DF3DF61CCCA1E4F2DCADFAC515BBCD
SHA-256:	91CB49C253F1E762A49AC001DD9B06F93D474F716BF3B7306E5C3DFAC37D9058
SHA-512:	6468FA16A4DFB3BA9B6E471A8BEFE155B99F2B7C965C1587CB69EA89774ACE7FA0F31D7E7084DBEDD03491DBDE316ABF1FC05BDA28250E967D5302A2532BF6D3
Malicious:	false
Preview:	MDMP..... .....<3.`.....U.....B.....T.....GenuineIntelW.....T.....4....2.`:.....0.....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\WERD677.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):	8400
Entropy (8bit):	3.695637388269918
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNioa6l296YSBSUGRfgmfGuSrCpBR89bVnqsfKHm:RrlsNid6l296Y0SUGRfgmfGuSfVnJfT
MD5:	C2E720B1A4E9CF17AF4E8ECEF455A2B7
SHA1:	750A0AA48D0E162F4D44B2CB3A4F65EB22C2B5CC
SHA-256:	39EF919FCEFCB20D2B89B7A4F398289638EBF94FC6BAFE003414EFD417A21A2F
SHA-512:	5EB1E91504FF55F7E4A3B61405C7A2FEAF15DCCBC44F7020B6A561B946784AF7ED0FBB7DCFB9FBC73207EB059725756A8773A0697C9A176A944C110E47254F9
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.>.2.1.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE76.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4753
Entropy (8bit):	4.4636931605483605
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtWI97TWSC8BS8fm8M4Jv6MFx+q8vc6ILJsGX7vXw3d:uITflgiSNRJSQKPILJsGX7vXgd
MD5:	8AB32FB89B7F98E921F5C34E2619C25B
SHA1:	759DA4A133E32560168AD5B71B57E82649A0BE9E
SHA-256:	B3E728D937C7FB31FE21BD337B07E0DB1880075618DAB584ECC3CD84CDD3DBCA
SHA-512:	BDA5D9F30B1ED21085ED93D89D9FF8BCF3BA9CC1FC858F43BB05CD8C5459A1623E2C1FDCE076F0AAA3904BDC8BD119FE2C546F479AB40F60CCF0B05A9984E086
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE76.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="816314" />.. <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\WERF661.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Jan 14 12:04:23 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	89920
Entropy (8bit):	1.9805037912276446
Encrypted:	false
SSDEEP:	384:ovZ6vbhAPkBGylxzXx3rrqw5ym1rPgY62EcOoEj0Gd2ol:P1APMGyXXNrYm1roYMoEIAl
MD5:	90409243EFAE234551EA1C01248C41D0
SHA1:	1AB4AC8A436E2CCE4D708C306504252552CB8092
SHA-256:	83AF683C5FD7E02271F18EF1280ECA5DDB688C5ACCB30AED591A17DE101B7550
SHA-512:	5B9C743BCBBD8742AAE5FC755475E03579AB649FCC37B47AFAA22A1A6F2E0999747518516ACCAE48B69343345AF089BB1F9D404503864AC989C11A92B445D70
Malicious:	false
Preview:	MDMP..... .....G3.`.....U.....B.....GenuineIntelW.....T.....4....2.`:.....0.....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..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.548995136814184
TrID:	• Win32 Executable (generic) a (10002005/4) 98.68% • Windows ActiveX control (116523/4) 1.15% • Windows Screen Saver (13104/52) 0.13% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	sample4.exe
File size:	2136576
MD5:	5009b8bcf024704c8b23e42c492f118c
SHA1:	df607367a88b5610a224909efb8debeb0d90f487
SHA256:	30f099660904079afcd445409cfd2eca735fab49dda522f0 3ed60d47f9f21bdc
SHA512:	70c4d7c6b9124246def27e28b69f2eb30bac85a5c0e8b38 cf593222bec02c561143ebf0995946d1c30ef5441a6152c f587ef2d70651482374017a321df1c8e3b
SSDEEP:	49152:o8X7Gl0vopNbyrbGhp475YHHmfjlzukdQ+ILi2k4 TmRB:Z4Gopkrbk4UHmfhzukfILi2k4Tm
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L....,0Y..... ....."....."....v!...@.....

File Icon



Icon Hash:	71c4b2f0e8d4c4c6

Static PE Info

General

Entrypoint:	0x11796e8
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x59302CB5 [Thu Jun 1 15:03:17 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	7da84c744589b5da0e6e3eb22df0b736

Entrypoint Preview

Instruction
call 00007FDD8C93D2C9h
jmp 00007FDD8C93C753h
jmp dword ptr [011D49B8h]
mov ecx, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], ecx
pop ecx
pop edi
pop edi
pop esi
pop ebx
mov esp, ebp
pop ebp
push ecx
ret
mov ecx, dword ptr [ebp-10h]
xor ecx, ebp
call 00007FDD8C93C08Ah
jmp 00007FDD8C93C8A0h
mov ecx, dword ptr [ebp-14h]
xor ecx, ebp
call 00007FDD8C93C079h
jmp 00007FDD8C93C88Fh
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [011B2F64h]
xor eax, ebp
push eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi

Instruction
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [011B2F64h]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1d49bc	0x168	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1f4000	0x17c2c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x20c000	0x1d2c0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x38f60	0x54	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x38fb4	0x18	.text
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2b670	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1d4000	0x9b8	.idata
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	0x1b02f4	0x1b0400	False	0.510258707165	data	6.51268656796	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1b2000	0x21d98	0x5c00	False	0.319166100543	data	5.12748414797	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x1d4000	0x3f8e	0x4000	False	0.398986816406	data	5.55581211033	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gfids	0x1d8000	0x19e58	0x1a000	False	0.296001727764	data	4.22633465795	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.giats	0x1f2000	0x10	0x200	False	0.05078125	data	0.155177575305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tls	0x1f3000	0x9	0x200	False	0.033203125	data	0.0203931352361	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1f4000	0x17c2c	0x17e00	False	0.248680873691	data	4.95227644363	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x20c000	0x1d2c0	0x1d400	False	0.432366786859	data	6.49808502841	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1f4370	0x94a8	data	English	United States
RT_ICON	0x1fd818	0x5488	data	English	United States
RT_ICON	0x202ca0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 15794175, next used block 4294905600	English	United States
RT_ICON	0x206ec8	0x25a8	data	English	United States
RT_ICON	0x209470	0x10a8	data	English	United States
RT_ICON	0x20a518	0x988	data	English	United States
RT_ICON	0x20aea0	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x20b308	0xb0	data	English	United States
RT_DIALOG	0x20b3b8	0xb8	data	English	United States
RT_STRING	0x20b470	0x82	data	English	United States
RT_STRING	0x20b4f4	0x1ba	data	English	United States
RT_STRING	0x20b6b0	0x54	data	English	United States
RT_GROUP_ICON	0x20b704	0x68	data	English	United States
RT_VERSION	0x20b76c	0x364	data	English	United States
RT_MANIFEST	0x20bad0	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
GDI32.dll	GetViewportOrgEx, GetWindowOrgEx, SetPixelV, SetPaletteEntries, ExtFloodFill, PtInRegion, GetBoundsRect, FrameRgn, FillRgn, GetTextFaceW, ScaleWindowExtEx, CreateCompatibleDC, CreateFontW, GetPixel, CreateRectRgn, SelectClipRgn, RoundRect, OffsetRgn, GetRgnBox, Rectangle, LPtoDP, CreateRoundRectRgn, Polyline, Polygon, CreatePolygonRgn, GetTextColor, Ellipse, CreateEllipticRgn, SetDIBColorTable, CreateDIBSection, StretchBlt, SetPixel, GetTextCharsetInfo, EnumFontFamiliesW, CreateDIBitmap, CreateCompatibleBitmap, GetBkColor, RealizePalette, GetSystemPaletteEntries, GetPaletteEntries, GetNearestPaletteIndex, CreatePalette, EnumFontFamiliesExW, GetTextMetricsW, DPtoLP, SetRectRgn, PatBlt, CreateRectRgnIndirect, CombineRgn, GetTextExtentPoint32W, ScaleViewportExtEx, OffsetWindowOrgEx, OffsetViewportOrgEx, SetWindowOrgEx, SetWindowExtEx, SetViewportOrgEx, SetViewportExtEx, CopyMetaFileW, CreateDCW, GetDeviceCaps, CreateBitmap, SetBkColor, SetTextColor, GetObjectW, DeleteObject, BitBlt, CreateHatchBrush, CreatePen, CreatePatternBrush, CreateSolidBrush, DeleteDC, Escape, ExcludeClipRect, GetClipBox, GetObjectType, GetStockObject, GetViewportExtEx, GetWindowExtEx, IntersectClipRect, LineTo, PtVisible, RectVisible, RestoreDC, SaveDC, ExtSelectClipRgn, SelectObject, SelectPalette, SetBkMode, SetMapMode, SetLayout, GetLayout, SetPolyFillMode, SetROP2, SetTextAlign, MoveToEx, TextOutW, ExtTextOutW, CreateFontIndirectW
KERNEL32.dll	FreeEnvironmentStringsW, GetConsoleMode, GetConsoleCP, HeapCreate, LCMapStringW, GetTimeZoneInformation, VirtualProtect, HeapFree, GetDiskFreeSpaceW, GetModuleFileNameW, InitializeCriticalSectionAndSpinCount, GetEnvironmentVariableW, CreateFileW, GetCurrentThreadId, HeapValidate, FindFirstChangeNotificationW, HeapSize, Sleep, GetLastError, HeapReAlloc, GetStdHandle, ExitProcess, GetFileType, SetStdHandle, QueryPerformanceFrequency, WriteConsoleW, GetStringTypeW, VirtualAlloc, GetCommandLineW, GetCommandLineA, HeapQueryInformation, GetModuleHandleExW, FreeLibraryAndExitThread, ExitThread, CreateThread, SetEnvironmentVariableW, RaiseException, GetEnvironmentStringsW, GetCPInfo, GetOEMCP, GetACP, IsValidCodePage, FindNextFileW, FindFirstFileExW, GetFileTime, FreeLibrary, GetProcessHeap, GetCurrentProcessId, DeleteCriticalSection, GetTimeFormatW, DecodePointer, HeapCompact, GetLocalTime, HeapAlloc, LoadLibraryW, GetSystemInfo, VirtualQuery, GetModuleHandleW, GetProcAddress, LoadLibraryExA, OutputDebugStringA, SetLastError, GetModuleHandleA, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GlobalAlloc, GlobalReAlloc, GlobalLock, GlobalHandle, GlobalUnlock, GlobalFree, LocalAlloc, LocalReAlloc, LocalFree, LoadResource, LockResource, SizeofResource, FindResourceW, WideCharToMultiByte, GlobalSize, MulDiv, FormatMessageW, CopyFileW, MultiByteToWideChar, CloseHandle, SetEvent, WaitForSingleObject, CreateEventW, SetThreadPriority, ResumeThread, lstrcmpA, GlobalGetAtomNameW, FileTimeToSystemTime, EncodePointer, GetSystemDirectoryW, FreeResource, LoadLibraryExW, GlobalDeleteAtom, lstrcmpW, LoadLibraryA, GlobalAddAtomW, GlobalFindAtomW, FindClose, FindFirstFileW, FlushFileBuffers, GetFileSize, GetFullPathNameW, GetVolumeInformationW, LockFile, ReadFile, SetEndOfFile, SetFilePointer, UnlockFile, WriteFile, DuplicateHandle, GetCurrentProcess, lstrcmpiW, CompareStringW, GetUserDefaultUILanguage, GlobalFlags, GetVersionExW, FileTimeToLocalFileTime, GetFileAttributesW, GetFileAttributesExW, GetFileSizeEx, SystemTimeToTzSpecificLocalTime, lstrcpyW, GetCurrentDirectoryW, FindResourceExW, GetWindowsDirectoryW, VerSetConditionMask, VerifyVersionInfoW, GetTempFileNameW, GetTempPathW, GetTickCount, GetProfileIntW, SearchPathW, ResetEvent, WaitForSingleObjectEx, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TerminateProcess, IsProcessorFeaturePresent, IsDebuggerPresent, GetStartupInfoW, QueryPerformanceCounter, GetSystemTimeAsFileTime, InitializeSListHead, OutputDebugStringW, RtlUnwind, SetFilePointerEx

DLL	Import
USER32.dll	UnhookWindowsHookEx, SendMessageW, EnableWindow, IsWindowEnabled, MessageBoxW, GetWindowLongW, GetParent, GetLastActivePopup, GetMenuStringW, GetSubMenu, GetMenuItemID, GetMenuItemCount, InsertMenuW, AppendMenuW, RemoveMenu, GetMessageW, TranslateMessage, DispatchMessageW, PeekMessageW, IsWindowVisible, GetActiveWindow, GetKeyState, ValidateRect, GetCursorPos, SetWindowsHookExW, CallNextHookEx, GetSystemMetrics, GetDC, ReleaseDC, GetSysColor, LoadCursorW, GetWindowTextW, GetWindowTextLengthW, GetFocus, CheckMenuItem, EnableMenuItem, SetMenuItemBitmaps, GetMenuCheckMarkDimensions, SetMenuItemInfoW, LoadBitmapW, RegisterWindowMessageW, GetMessagePos, GetMessageTime, PostMessageW, DefWindowProcW, CallWindowProcW, RegisterClassW, GetClassInfoW, GetClassInfoExW, CreateWindowExW, IsWindow, IsMenu, IsChild, DestroyWindow, SetWindowPos, GetWindowPlacement, SetWindowPlacement, BeginDeferWindowPos, DeferWindowPos, EndDeferWindowPos, IsIconic, GetDlgItem, GetDlgCtrlID, SetFocus, GetCapture, GetMenu, SetMenu, TrackPopupMenu, UpdateWindow, SetActiveWindow, SetForegroundWindow, BeginPaint, EndPaint, RedrawWindow, ScrollWindow, SetScrollPos, GetScrollPos, SetScrollRange, GetScrollRange, ShowScrollBar, SetPropW, GetPropW, RemovePropW, AdjustWindowRectEx, ScreenToClient, MapWindowPoints, CopyRect, EqualRect, PtInRect, SetWindowLongW, GetClassLongW, GetClassNameW, GetTopWindow, GetWindow, LoadIconW, SetScrollInfo, GetScrollInfo, WinHelpW, MonitorFromWindow, GetMonitorInfoW, ShowWindow, MoveWindow, CheckDlgButton, GetWindowThreadProcessId, SetWindowTextW, IsDialogMessageW, DestroyIcon, CharUpperW, ClientToScreen, GetDesktopWindow, RealChildWindowFromPoint, DrawTextW, DrawTextExW, GrayStringW, TabbedTextOutW, GetWindowDC, FillRect, DestroyMenu, GetMenuItemInfoW, InflateRect, SystemParametersInfoW, CopyImage, SendDlgItemMessageA, SetRectEmpty, OffsetRect, PostQuitMessage, EndDialog, GetNextDlgTabItem, GetAsyncKeyState, MapDialogRect, IntersectRect, TrackMouseEvent, InvalidateRect, LoadImageW, ShowOwnedPopups, SetCursor, DeleteMenu, SetTimer, KillTimer, GetNextDlgGroupItem, SetCapture, ReleaseCapture, WindowFromPoint, DrawFocusRect, IsRectEmpty, DrawIconEx, GetIconInfo, MessageBeep, EnableScrollBar, HideCaret, InvertRect, NotifyWinEvent, GetMenuDefaultItem, MapVirtualKeyW, GetKeyNameTextW, LoadMenuW, SetLayeredWindowAttributes, EnumDisplayMonitors, SetClassLongW, SetWindowRgn, SetParent, OpenClipboard, CloseClipboard, SetClipboardData, EmptyClipboard, DrawStateW, DrawEdge, DrawFrameControl, IsZoomed, GetSystemMenu, BringWindowToTop, SetCursorPos, CopyIcon, FrameRect, DrawIcon, UnionRect, UpdateLayeredWindow, MonitorFromPoint, LoadAcceleratorsW, TranslateAcceleratorW, InsertMenuItemW, UnpackDDElParam, ReuseDDElParam, GetComboBoxInfo, PostThreadMessageW, WaitMessage, GetKeyboardLayout, IsCharLowerW, MapVirtualKeyExW, ToUnicodeEx, GetKeyboardState, CreateAcceleratorTableW, DestroyAcceleratorTable, CopyAcceleratorTableW, SetRect, LockWindowUpdate, SetMenuDefaultItem, GetDoubleClickTime, ModifyMenuW, RegisterClipboardFormatW, CharUpperBuffW, IsClipboardFormatAvailable, GetUpdateRect, DrawMenuBar, DefFrameProcW, DefMDIChildProcW, TranslateMDISysAccel, SubtractRect, CreateMenu, GetWindowRgn, DestroyCursor, GetWindowRect, CreatePopupMenu, GetForegroundWindow, DialogBoxIndirectParamW, GetClientRect, GetSysColorBrush, CreateDialogIndirectParamW, GetMenuState
COMCTL32.dll	ImageList_SetOverlayImage, CreateStatusWindowW, CreateToolbarEx, DestroyPropertySheetPage, ImageList_LoadImageW
COMDLG32.dll	GetFileTitleW, GetSaveFileNameW, FindTextW, GetOpenFileNameW
ole32.dll	CoInitializeEx, IsAccelerator, OleTranslateAccelerator, OleDestroyMenuDescriptor, OleCreateMenuDescriptor, OleLockRunning, RevokeDragDrop, RegisterDragDrop, CoLockObjectExternal, OleGetClipboard, DoDragDrop, CreateStreamOnHGlobal, CoCreateInstance, CoDisconnectObject, ReleaseStgMedium, OleDuplicateData, CoTaskMemFree, CoTaskMemAlloc, CoRevokeClassObject, OleInitialize, CoUninitialize, OleSetContainedObject, CoInitialize, OleUninitialize
WS2_32.dll	setsockopt, WSACleanup, WSACloseEvent, WSACreateEvent, getprotobynumber, WSAStartup, WSAConnect, socket, WSAAddressToStringW, getservbyname
WININET.dll	InternetCanonicalizeUrlW, InternetOpenUrlW, InternetWriteFile, InternetOpenW, InternetReadFile, InternetCloseHandle, InternetQueryDataAvailable, InternetCrackUrlW, InternetSetFilePointer, HttpQueryInfoW
SHLWAPI.dll	PathCanonicalizeW, PathIsRootW, StrCmpW, StrFormatKBSizeW, PathRemoveFileSpecW, PathFindExtensionW, PathStripToRootW, SHCreateStreamOnFileW, PathIsUNCW, PathFindFileNameW
UxTheme.dll	GetThemeTextExtent, DrawThemeText, DrawThemeParentBackground, OpenThemeData, GetThemeBackgroundRegion, CloseThemeData, DrawThemeBackground, GetThemePartSize, GetThemeSysColor, IsThemeBackgroundPartiallyTransparent, IsAppThemed, GetWindowTheme, GetCurrentThemeName, GetThemeColor
IMM32.dll	ImmGetContext, ImmReleaseContext, ImmSetCompositionFontW, ImmSetCompositionWindow, ImmGetCompositionStringW, ImmNotifyIME, ImmGetOpenStatus
WINSPOOL.DRV	ClosePrinter, DocumentPropertiesW, OpenPrinterW
OLEACC.dll	AccessibleObjectFromWindow, LresultFromObject, CreateStdAccessibleObject
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteW, SHGetFileInfoW, SHAppBarMessage, SHBrowseForFolderW, DragFinish, DragQueryFileW, SHGetPathFromIDListW, SHGetDesktopFolder
gdiplus.dll	GdipDrawImageRectI, GdipSetInterpolationMode, GdipCreateFromHDC, GdipCreateBitmapFromHBITMAP, GdipDrawImageI, GdipDeleteGraphics, GdipBitmapUnlockBits, GdipBitmapLockBits, GdipCreateBitmapFromScan0, GdipCreateBitmapFromStream, GdipGetImagePaletteSize, GdipGetImagePalette, GdipGetImagePixelFormat, GdipGetImageHeight, GdipGetImageWidth, GdipGetImageGraphicsContext, GdipCloneImage, GdiplusStartup, GdipFree, GdipAlloc, GdiplusShutdown, GdipDisposeImage
ADVAPI32.dll	RegDeleteValueW, RegCreateKeyExW, RegDeleteKeyW, RegOpenKeyExW, RegQueryValueExW, RegSetValueExW, RegEnumKeyExW, RegCloseKey
MSIMG32.dll	TransparentBlt, AlphaBlend

Version Infos

Description	Data
LegalCopyright	Column tell Corporation. All rights reserved.
InternalName	arra.exe
FileVersion	10.7.14.75 built by: 39959
CompanyName	Column tell Corporation
ProductName	Column tell Column tell 2014
ProductVersion	10.7.14.75

Description	Data
FileDescription	Column tell Nine in
OriginalFilename	arra.exe
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



Total Packets: 79

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 04:05:17.927963018 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:17.968168020 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:17.968981028 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:17.971504927 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.011701107 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.012576103 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.012602091 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.012618065 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.012722015 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.022810936 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.062938929 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.063695908 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.069999933 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.110133886 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.223429918 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.226116896 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.266465902 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.385466099 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.385489941 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.385500908 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.385516882 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.385529995 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.385548115 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.385560989 CET	443	49761	104.244.42.131	192.168.2.3

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 04:05:18.385569096 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.385586023 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.385592937 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.385724068 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.425858021 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.425884962 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.425900936 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.425925016 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.425942898 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.425960064 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.425976992 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.425988913 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.425993919 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.426012993 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.426023006 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.426028967 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.426043987 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.426050901 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.426063061 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.426080942 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.426083088 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.426096916 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.426112890 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.426115990 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.426127911 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.426145077 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.426147938 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.426160097 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.426176071 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.426178932 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.426197052 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.426203966 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.426253080 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.466248035 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466281891 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466303110 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466329098 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466351986 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466372967 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466384888 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.466394901 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466417074 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466428041 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.466438055 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466454983 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.466459990 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466480970 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466507912 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466509104 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.466531038 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466551065 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466573000 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466593981 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466614008 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466640949 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.466643095 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466662884 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466682911 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.466687918 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466710091 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466730118 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466734886 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.466751099 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466772079 CET	443	49761	104.244.42.131	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 04:05:18.466778994 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.466790915 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466815948 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466835022 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466839075 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.466861010 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466885090 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466886044 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.466905117 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466912985 CET	49761	443	192.168.2.3	104.244.42.131
Jan 14, 2021 04:05:18.466926098 CET	443	49761	104.244.42.131	192.168.2.3
Jan 14, 2021 04:05:18.466944933 CET	49761	443	192.168.2.3	104.244.42.131

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 04:02:42.073015928 CET	60100	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:02:42.132333994 CET	53	60100	8.8.8.8	192.168.2.3
Jan 14, 2021 04:02:43.212511063 CET	53195	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:02:43.268817902 CET	53	53195	8.8.8.8	192.168.2.3
Jan 14, 2021 04:02:44.586344004 CET	50141	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:02:44.637275934 CET	53	50141	8.8.8.8	192.168.2.3
Jan 14, 2021 04:02:45.816457987 CET	53023	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:02:45.874295950 CET	53	53023	8.8.8.8	192.168.2.3
Jan 14, 2021 04:02:46.975577116 CET	49563	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:02:47.034167051 CET	53	49563	8.8.8.8	192.168.2.3
Jan 14, 2021 04:02:48.168927908 CET	51352	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:02:48.216887951 CET	53	51352	8.8.8.8	192.168.2.3
Jan 14, 2021 04:02:49.390399933 CET	59349	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:02:49.438287020 CET	53	59349	8.8.8.8	192.168.2.3
Jan 14, 2021 04:02:50.543476105 CET	57084	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:02:50.591331959 CET	53	57084	8.8.8.8	192.168.2.3
Jan 14, 2021 04:02:51.763727903 CET	58823	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:02:51.811760902 CET	53	58823	8.8.8.8	192.168.2.3
Jan 14, 2021 04:02:53.013219118 CET	57568	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:02:53.061137915 CET	53	57568	8.8.8.8	192.168.2.3
Jan 14, 2021 04:02:55.540607929 CET	50540	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:02:55.599895954 CET	53	50540	8.8.8.8	192.168.2.3
Jan 14, 2021 04:02:56.658823967 CET	54366	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:02:56.715101957 CET	53	54366	8.8.8.8	192.168.2.3
Jan 14, 2021 04:02:57.587508917 CET	53034	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:02:57.635356903 CET	53	53034	8.8.8.8	192.168.2.3
Jan 14, 2021 04:03:13.865518093 CET	57762	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:03:14.008744955 CET	53	57762	8.8.8.8	192.168.2.3
Jan 14, 2021 04:03:28.355820894 CET	55435	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:03:28.413849115 CET	53	55435	8.8.8.8	192.168.2.3
Jan 14, 2021 04:03:28.958537102 CET	50713	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:03:29.009180069 CET	53	50713	8.8.8.8	192.168.2.3
Jan 14, 2021 04:03:30.788479090 CET	56132	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:03:30.849518061 CET	53	56132	8.8.8.8	192.168.2.3
Jan 14, 2021 04:03:40.658459902 CET	58987	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:03:40.716289997 CET	53	58987	8.8.8.8	192.168.2.3
Jan 14, 2021 04:03:50.941011906 CET	56579	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:03:51.012018919 CET	53	56579	8.8.8.8	192.168.2.3
Jan 14, 2021 04:04:06.841526031 CET	60633	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:04:06.899365902 CET	53	60633	8.8.8.8	192.168.2.3
Jan 14, 2021 04:04:07.443937063 CET	61292	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:04:07.492047071 CET	53	61292	8.8.8.8	192.168.2.3
Jan 14, 2021 04:04:07.621474028 CET	63619	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:04:07.670430899 CET	53	63619	8.8.8.8	192.168.2.3
Jan 14, 2021 04:04:11.022910118 CET	64938	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:04:11.087511063 CET	53	64938	8.8.8.8	192.168.2.3
Jan 14, 2021 04:04:15.723376989 CET	61946	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:04:15.792798996 CET	53	61946	8.8.8.8	192.168.2.3

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 04:04:17.913858891 CET	64910	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:04:17.962712049 CET	53	64910	8.8.8.8	192.168.2.3
Jan 14, 2021 04:04:28.063801050 CET	52123	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:04:28.114609957 CET	53	52123	8.8.8.8	192.168.2.3
Jan 14, 2021 04:04:39.059943914 CET	56130	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:04:39.119180918 CET	53	56130	8.8.8.8	192.168.2.3
Jan 14, 2021 04:04:39.410049915 CET	56338	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:04:39.468117952 CET	53	56338	8.8.8.8	192.168.2.3
Jan 14, 2021 04:04:44.425735950 CET	59420	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:04:44.473823071 CET	53	59420	8.8.8.8	192.168.2.3
Jan 14, 2021 04:04:49.251020908 CET	58784	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:04:49.298911095 CET	53	58784	8.8.8.8	192.168.2.3
Jan 14, 2021 04:04:52.946593046 CET	63978	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:04:53.006309986 CET	53	63978	8.8.8.8	192.168.2.3
Jan 14, 2021 04:04:58.881520987 CET	62938	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:04:58.943303108 CET	53	62938	8.8.8.8	192.168.2.3
Jan 14, 2021 04:04:59.224991083 CET	55708	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:04:59.645874023 CET	53	55708	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:00.050563097 CET	56803	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:00.277928114 CET	53	56803	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:05.585212946 CET	57145	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:05.944235086 CET	53	57145	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:11.815483093 CET	55359	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:11.878107071 CET	53	55359	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:17.850574970 CET	58306	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:17.915168047 CET	53	58306	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:20.444683075 CET	64124	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:20.492532015 CET	53	64124	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:20.922383070 CET	49361	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:20.990811110 CET	53	49361	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:24.093696117 CET	63150	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:24.167789936 CET	53	63150	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:31.951855898 CET	53279	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:32.100008011 CET	53	53279	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:32.717174053 CET	56881	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:32.827061892 CET	53	56881	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:34.039890051 CET	53642	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:34.096226931 CET	53	53642	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:34.543354034 CET	55667	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:34.602196932 CET	53	55667	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:35.091520071 CET	54833	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:35.147965908 CET	53	54833	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:35.698450089 CET	62476	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:35.754991055 CET	53	62476	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:36.282718897 CET	49705	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:36.339052916 CET	53	49705	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:36.981055975 CET	61477	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:37.040271997 CET	53	61477	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:37.704214096 CET	61633	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:37.760768890 CET	53	61633	8.8.8.8	192.168.2.3
Jan 14, 2021 04:05:38.128257990 CET	55949	53	192.168.2.3	8.8.8.8
Jan 14, 2021 04:05:38.188183069 CET	53	55949	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 04:04:11.022910118 CET	192.168.2.3	8.8.8.8	0x3dd2	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Jan 14, 2021 04:04:39.410049915 CET	192.168.2.3	8.8.8.8	0xc9d	Standard query (0)	support.oracle.com	A (IP address)	IN (0x0001)
Jan 14, 2021 04:04:52.946593046 CET	192.168.2.3	8.8.8.8	0xb677	Standard query (0)	www.oracle.com	A (IP address)	IN (0x0001)
Jan 14, 2021 04:04:58.881520987 CET	192.168.2.3	8.8.8.8	0x617f	Standard query (0)	www.intel.com	A (IP address)	IN (0x0001)
Jan 14, 2021 04:04:59.224991083 CET	192.168.2.3	8.8.8.8	0xa65d	Standard query (0)	www.intel.ch	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 04:05:00.050563097 CET	192.168.2.3	8.8.8.8	0x23d9	Standard query (0)	corpredirect.intel.com	A (IP address)	IN (0x0001)
Jan 14, 2021 04:05:05.585212946 CET	192.168.2.3	8.8.8.8	0x264b	Standard query (0)	gegemony4you.top	A (IP address)	IN (0x0001)
Jan 14, 2021 04:05:17.850574970 CET	192.168.2.3	8.8.8.8	0x9598	Standard query (0)	help.twitter.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 04:03:28.413849115 CET	8.8.8.8	192.168.2.3	0x99f8	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:04:06.899365902 CET	8.8.8.8	192.168.2.3	0x4b41	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:04:11.087511063 CET	8.8.8.8	192.168.2.3	0x3dd2	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:04:39.468117952 CET	8.8.8.8	192.168.2.3	0xc9d	No error (0)	support.oracle.com	support.oracle.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:04:53.006309986 CET	8.8.8.8	192.168.2.3	0xb677	No error (0)	www.oracle.com	ds-www.oracle.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:04:58.943303108 CET	8.8.8.8	192.168.2.3	0x617f	No error (0)	www.intel.com	intel11.cn.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:04:59.645874023 CET	8.8.8.8	192.168.2.3	0xa65d	No error (0)	www.intel.ch	intel19233.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:05:00.277928114 CET	8.8.8.8	192.168.2.3	0x23d9	No error (0)	corpredirect.intel.com	intel11.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:05:05.944235086 CET	8.8.8.8	192.168.2.3	0x264b	Name error (3)	gegemony4you.top	none	none	A (IP address)	IN (0x0001)
Jan 14, 2021 04:05:17.915168047 CET	8.8.8.8	192.168.2.3	0x9598	No error (0)	help.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2021 04:05:17.915168047 CET	8.8.8.8	192.168.2.3	0x9598	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
Jan 14, 2021 04:05:17.915168047 CET	8.8.8.8	192.168.2.3	0x9598	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
Jan 14, 2021 04:05:17.915168047 CET	8.8.8.8	192.168.2.3	0x9598	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Jan 14, 2021 04:05:17.915168047 CET	8.8.8.8	192.168.2.3	0x9598	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)

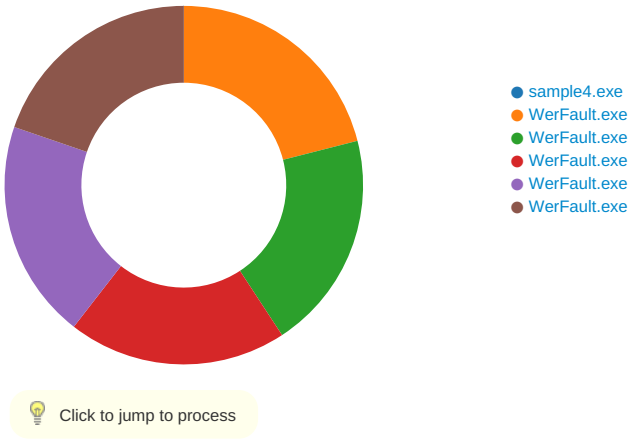
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 14, 2021 04:05:18.012618065 CET	104.244.42.131	443	192.168.2.3	49761	CN=*.twitter.com, OU=fra2, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Mar 05 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Mar 02 13:00:00 CET 2021 Sun Oct 22 14:00:00 CEST 2028	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=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: sample4.exe PID: 2100 Parent PID: 5880

General

Start time:	04:02:46
Start date:	14/01/2021
Path:	C:\Users\user\Desktop\sample4.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\sample4.exe'
Imagebase:	0xd0000
File size:	2136576 bytes
MD5 hash:	5009B8BCF024704C8B23E42C492F118C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_IcedID_3, Description: Yara detected IcedID, Source: 00000000.00000003.362692606.0000000001320000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_3, Description: Yara detected IcedID, Source: 00000000.00000002.551228989.00000000000D1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 1488 Parent PID: 2100

General

Start time:	04:04:00
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2100 -s 768
Imagebase:	0x9e0000
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	6E4D1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB592.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB592.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_058db978	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_058db978\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E4C497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB592.tmp	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB592.tmp.xml	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.csv	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB86F.tmp.txt	success or wait	1	6E4C497A	unknown

File Written

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 34 33 00 60 a4 05 12 00 00 00 00 00	MDMP........ ....43.`........	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.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 f4 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 34 08 00 00 e6 32 00 60 3a 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 0d 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 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... ....4....2.`:................. ....0.................. 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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.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 89 6c 24 24 ac f6 45 03 00 00 00 00 00 00 0d 00 89 6c 24 24 00 00 00 00 b8 f6 45 03 89 6c 24 24 23 00 00 00 46 02 01 00 9c f6 45 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	....+...S...+. ..+....l$$..E..........l$$.... ..E..l$$#...F.....E.+.........	success or wait	1	6E4C497A	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp</td><td>unknown</td><td>168</td><td>30 17 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 89 6c 24 24 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 89 6c 24 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 9c 24 00 00</td><td>0........................l$$..
..................l$$........
....
....
....
...............$..</td><td>success or wait</td><td>1</td><td>6E4C497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp</td><td>unknown</td><td>20</td><td>1e 00 00 00 bc e8 45 03 00 00 00 00 44 17 00 00 48 37 00 00</td><td>......E.....D...H7..</td><td>success or wait</td><td>30</td><td>6E4C497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp</td><td>unknown</td><td>5956</td><td>bc 9a e5 77 f2 1d ea 77 aa aa aa aa f0 e8 45 03 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 48 ee 45 03 00 00 00 00 fc 02 00 00 00 00 00 00 00 00 00 00 fc 02 00 00 24 03 00 00 88 e9 45 03 aa aa aa aa 88 e9 45 03 12 12 ea 77 24 03 00 00 00 00 00 00 aa aa aa aa ec e9 45 03 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 7c eb 45 03 2c eb 45 03 24 03 00 00 00 00 37 01 04 00 00 00 00 03 00 00 08 03 00 00 04 03 00 00 fc 02 00 00 00 00 00 00 fc 02 00 00 00 03 00 00 04 03 00 00 08 03 00 00 aa aa aa aa 10 e9 45 03 aa aa aa aa 3c ea 45 03 f0 17 e6 77 aa aa aa aa 00 00 00 00 a4 e9 45 03 91 0c ea 77 aa aa aa aa 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 4c f7 45 03 3d ac e9 77 2c eb 45 03 7c eb 45 03 aa aa aa aa 00 00 00</td><td>...w...w......E...............
..H.E.....................$...
..E.......E....w$.............
E.............................
|.E.,.E.$.....7...............
................................E.....
<.E....w..........E...
.w....................L.E.=..w
,.E.|.E........</td><td>success or wait</td><td>29</td><td>6E4C497A</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp	unknown	1196	bc b1 e5 77 d6 c9 e3 77 b4 00 00 00 aa aa aa aa 10 00 00 00 e8 fb 71 01 b4 fc 71 01 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 d0 11 01 00 d0 11 01 00 00 00 00 b4 00 00 00 aa aa aa aa b4 00 00 00 aa aa aa aa 00 d0 11 01 00 00 00 00 00 00 00 00 00 00 00 00 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 aa aa aa aa f0 90 48 01 00 00 00 00 00 00 00 00 18 69 45 01 00 b0 10 01 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 44 fc 81 01 d4 fb 34 03 4c fc 81 01 88 6d 45 01 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.............q...q... ..@..w@..w................... ....H... ....iE.................... ....D..... 4.L....mE....................	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp	unknown	4	05 00 00 00	....	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.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 dc 02 00 00 00 00 00 00 60 f4 2f 01 00 00 00 00 00 00 00 00 00 00 00 00 80 f3 2f 01 2c 95 e5 77 23 00 00 00 12 02 00 00 10 f3 2f 01 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#........./.+.........	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp	unknown	48	30 17 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 30 12 01 00 00 00 00 bc e8 45 03 00 00 00 00 44 17 00 00 48 37 00 00 cc 02 00 00 98 32 00 00	0....... ....0........E... ..D...H7.......2..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp	unknown	4	30 00 00 00	0...	success or wait	48	6E4C497A	unknown

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp	unknown	28	16 00 00 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 00 2e 00 65 00 78 00 65 00 00 00	....s.a.m.p.l.e.4...e.x.e...	success or wait	48	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp	unknown	120	00 00 8b 75 00 00 00 00 00 70 00 00 07 dc 00 00 28 63 3e 35 4c 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 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 01 00 00 00	...u.....p......(c>5L$..... ....B.......B?..... ....@E.....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n .R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp	unknown	668	00 00 7e 73 00 00 00 00 00 10 01 00 03 ab 01 00 c4 1f 6d 8d 60 24 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 00 01 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 30 f7 01 00 00 00 00 00 60 af 02 00 00 00 00 8b 64 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 97 26 01 00 00 00 00 00 fc 5e 03 00 00 00 00 00 4f 78 02 00 00 00 00 00 f2 9d 1b 00 00 00 00 00 4e 61 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 64 71 12 00 00 00 00 00 20 b0 ce 51 00 00 00 00 59 e6 22 20 00 00 00 00 4a c7 f6 0d 00 00 00 00 f3 90 e8 00 00 00 00 00 1e b5 00 00 4b d2 00 00 f1 42 05 00 ed 81 0b 00 4e 61 04 00 fb 7e 15 00 64 71 12 00 15 00 3a 00 f6 35 01 00 de fa 15 00 00 00 00 00 35 63 24 00 75 a2 04	..~s.....m.`$.....Zb ..... .....0.....` .....d.....&.. .....^.....Ox.....Na .....@.....dq..... ..Q....Y." ....J.....K. ...B.....Na...~..dq....:..5.. .....5c$.u..	success or wait	1	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp	unknown	10978	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 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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERABCC.tmp.dmp	unknown	120	03 00 00 00 f4 00 00 00 08 07 00 00 04 00 00 00 44 14 00 00 08 08 00 00 0e 00 00 00 24 00 00 00 4c 1c 00 00 05 00 00 00 e4 01 00 00 64 35 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 88 1e 00 00 de cd 00 00 15 00 00 00 ec 01 00 00 70 1c 00 00 16 00 00 00 98 00 00 00 5c 1e 00 00	.....D.....$...L.....d5.....`....8.....T.....p.....\...	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 31 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.1.0.0.<./.P.i.d.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	68	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 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.a.m.p.l.e.4...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 38 00 31 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.>.7.8.1.1.2.<./.U.p.t.i.m.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 31 00 33 00 33 00 39 00 31 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.>.1.0.1.3.3.9.1.3.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 31 00 33 00 33 00 30 00 39 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.>.1.0.1.3.3.0.9.4.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 32 00 39 00 34 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.>.2.9.4.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 31 00 32 00 32 00 37 00 31 00 33 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.>.1.1.2.2.7.1.3.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 31 00 32 00 32 00 37 00 31 00 33 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.>.1.1.2.2.7.1.3.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 39 00 32 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.>.1.8.9.2.8.0.<./.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 38 00 34 00 30 00 38 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.>.1.8.8.4.0.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 32 00 38 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 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.>.2.8.3.6.8.<./.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 32 00 38 00 30 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.>.2.8.0.9.6.<./.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 32 00 32 00 33 00 32 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.>.2.2.3.2.3.2.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 32 00 32 00 34 00 30 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.>.2.2.4.0.5.1.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 32 00 32 00 33 00 32 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.>.2.2.3.2.3.2.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.3.8.8.<./.P.i.d.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 31 00 33 00 39 00 32 00 36 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.>.6.1.3.9.2.6.0.<./.U.p.t.i.m.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 35 00 39 00 38 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.>.5.5.9.8.3.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 35 00 33 00 34 00 35 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.>.1.0.5.3.4.5.0.2.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 39 00 38 00 36 00 30 00 33 00 30 00 30 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.>.9.8.6.0.3.0.0.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 37 00 37 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.>.9.7.7.6.8.8.<./.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	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 38 00 39 00 30 00 39 00 37 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.>.8.9.0.9.7.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 33 00 34 00 30 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.>.7.3.4.0.8.<./.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 36 00 34 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.>.6.8.6.4.8.<./.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 32 00 39 00 37 00 34 00 35 00 31 00 35 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.>.2.9.7.4.5.1.5.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 33 00 31 00 38 00 36 00 35 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.>.3.7.3.1.8.6.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 32 00 39 00 37 00 34 00 35 00 31 00 35 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.>.2.9.7.4.5.1.5.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 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.>.B.E.X.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 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.a.m.p.l.e.4...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 79 00 67 00 63 00 6f 00 70 00 78 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.>.y.g.c.o.p.x.,. .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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 79 00 67 00 63 00 6f 00 70 00 78 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.>.y.g.c.o.p.x.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 35 00 39 00 32 00 39 00 31 00 32 00 38 00 35 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.>.1.5.5.9.2.9.1.2.8.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 31 00 2d 00 31 00 34 00 54 00 31 00 32 00 3a 00 30 00 34 00 3a 00 30 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.-.0.1.-.1.4.T.1.2.:.0.4.:.0.4.Z.".>.	success or wait	1	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	266	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 33 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 31 00 30 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 37 00 33 00 30 00 34 00 36 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 37 00 33 00 30 00 34 00 36 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.3.9.". .P.I.D.=.".2.1.0.0.". .U.p.t.i.m.e.M.S.=.".7.3.0.4. 6.". .T.i.m.e.S.i.n.c.e.C.r.e. a.t.i.o.n.M.S.=.".7.3.0.4.6.". .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	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 65 00 63 00 61 00 31 00 36 00 36 00 30 00 2d 00 32 00 36 00 31 00 30 00 2d 00 34 00 31 00 65 00 38 00 2d 00 62 00 38 00 34 00 32 00 2d 00 35 00 30 00 64 00 33 00 65 00 32 00 33 00 36 00 33 00 61 00 66 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.9.e.c.a.1.6.6.0.-.2.6.1.0.-.4.1.e.8.-.b.8.4.2.-.5.0.d.3.e.2.3.6.3.a.f.2.<./.G.u.i.d.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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 31 00 2d 00 31 00 34 00 54 00 31 00 32 00 3a 00 30 00 34 00 3a 00 30 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.-.0.1.-.1.4.T.1.2.:.0.4.:.0.4.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3DB.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	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB592.tmp.xml	unknown	4753	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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_058db978\Report.wer	unknown	2	ff fe	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_058db978\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	174	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_058db978\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 31 00 35 00 32 00 31 00 33 00 38 00 32 00 38 00 39 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.5.2.1.3.8.2.8.9.	success or wait	1	6E4C497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	success or wait	1	6E4E36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6E4E1FB2	RegCreateKeyExW
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E4C43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	ProgramId	unicode	0006b8afee81a75154cbbd8a0ff7c2f6369d00000904	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	FileId	unicode	0000df607367a88b5610a224909efb8debeb0d90f487	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	LowerCaseLongPath	unicode	c:\users\user\desktop\sample4.exe	success or wait	1	6E4E36BF	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	LongPathHash	unicode	sample4.exe|f84237dc	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	Name	unicode	sample4.exe	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	Publisher	unicode	column tell corporation	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	Version	unicode	10.7.14.75 built by: 39959	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	BinFileVersion	unicode	10.7.14.75	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	BinaryType	unicode	pe32_i386	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	ProductName	unicode	column tell .column tell . 2014	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	ProductVersion	unicode	10.7.14.75	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	LinkDate	unicode	06/01/2017 15:03:17	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	BinProductVersion	unicode	10.7.14.75	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	Size	B	00 9A 20 00 00 00 00 00	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	Language	dword	1033	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	IsPeFile	dword	1	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{8f7ef7c7-838e-10aa-ff47-6d2853fe9509}\Root\InventoryApplicationFile\sample4.exe|f84237dc	IsOsComponent	dword	0	success or wait	1	6E4E36BF	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 89 6C 24 24 02 00 00 00 08 00 00 00 89 6C 24 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6E4E1FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 5920 Parent PID: 2100

General

Start time:	04:04:08
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2100 -s 804
Imagebase:	0x9e0000
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	6E4D1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE76.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE76.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_177de25c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_177de25c\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E4C497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE76.tmp	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE76.tmp.xml	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE86.tmp.csv	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1B4.tmp.txt	success or wait	1	6E4C497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 3c 33 00 60 a4 05 12 00 00 00 00 00	MDMP..... .....<3.`.....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.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 54 1f 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 34 08 00 00 e6 32 00 60 3a 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 0d 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......T..... ..GenuineIntelW...........T... ....4....2.`:................. ....0.................. 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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.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 89 6c 24 24 f4 f8 8e 03 00 00 00 00 00 00 0d 00 89 6c 24 24 00 00 00 00 00 f9 8e 03 89 6c 24 24 23 00 00 00 46 02 01 00 e4 f8 8e 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...+. ..+....l$$.............l$$.... .....l$$#...F.......+.........	success or wait	1	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	168	9c 04 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 89 6c 24 24 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 89 6c 24 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 fc 24 00 00	.........................l$$.. ....l$$........ ....$..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	20	2e 00 00 00 54 f9 45 03 00 00 00 00 ac 06 00 00 40 3e 00 00	....T.E.........@>..	success or wait	46	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	1708	bc b1 e5 77 d6 c9 e3 77 e8 02 00 00 aa aa aa aa 10 00 00 00 e8 f9 45 03 b4 fa 45 03 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa aa aa aa aa 00 00 00 00 78 6d 4a 01 e8 02 00 00 aa aa aa aa e8 02 00 00 aa aa aa aa aa aa aa aa 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 aa aa aa aa 28 51 49 01 00 00 00 00 00 00 00 00 50 8e 46 01 00 b0 10 01 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 54 b2 10 01 44 fc 81 01 f0 2a 49 01 f0 2a 49 01 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.............E...E... ..@..w@..w............xmJ..... ....(QI... ......P.F..................... ........................T...D. ...*I..*I.....................	success or wait	45	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	1196	bc b1 e5 77 d6 c9 e3 77 b4 00 00 00 aa aa aa aa 10 00 00 00 e8 fb 71 01 b4 fc 71 01 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 d0 11 01 00 d0 11 01 00 00 00 00 b4 00 00 00 aa aa aa aa b4 00 00 00 aa aa aa aa 00 d0 11 01 00 00 00 00 00 00 00 00 00 00 00 00 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 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa f0 90 48 01 00 00 00 00 00 00 00 00 18 69 45 01 00 b0 10 01 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 44 fc 81 01 d4 fb 34 03 4c fc 81 01 88 6d 45 01 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..............q...q... ..@..w@..w.................... ....H... ....iE..................... ....D..... 4.L....mE.....................	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	4	07 00 00 00	....	success or wait	7	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.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 00 80 7b f0 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 c3 2f 01 2c 95 e5 77 23 00 00 00 06 02 00 00 b8 c3 2f 01 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................ ../.,..w#........./.+.........	success or wait	7	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	48	dc 0c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 90 12 01 00 00 00 00 fc fa 9e 03 00 00 00 00 04 05 00 00 ec 44 00 00 cc 02 00 00 90 38 00 00	....D.......8..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	4	30 00 00 00	0...	success or wait	48	6E4C497A	unknown

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	28	16 00 00 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 00 2e 00 65 00 78 00 65 00 00 00	....s.a.m.p.l.e.4...e.x.e...	success or wait	48	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	120	00 00 8b 75 00 00 00 00 00 70 00 00 07 dc 00 00 28 63 3e 35 ac 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 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 01 00 00 00	...u.....p......(c>5.$..... .....B.....B?..... ....@E.....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n .R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	668	00 00 7e 73 00 00 00 00 00 10 01 00 03 ab 01 00 c4 1f 6d 8d c0 24 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 00 01 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 60 f1 01 00 00 00 00 00 60 af 02 00 00 00 00 1c 66 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 bd 2c 01 00 00 00 00 00 fc 5e 03 00 00 00 00 00 4f 78 02 00 00 00 00 00 dd 6b 1b 00 00 00 00 00 63 93 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 64 71 12 00 00 00 00 00 a0 73 98 53 00 00 00 00 26 fc ff 21 00 00 00 00 2c a5 44 0e 00 00 00 00 2b 9a ff 00 00 00 00 00 a3 b8 00 00 a1 e9 00 00 8f 84 05 00 2a 57 0b 00 63 93 04 00 fb 7e 15 00 64 71 12 00 bb 9b 3c 00 c5 3c 01 00 24 44 17 00 00 00 00 00 0d d9 25 00 27 a9 04	..~s.....m..$.....Zb ....`.....` .....f.....,.. .....^.....Ox.....k.....c. .....@.....dq.....s.S.... &..!....,.D.....+..... .....*W..c....~..dq....<..<.. $D.....%.'..	success or wait	1	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	13520	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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB79.tmp.dmp	unknown	120	03 00 00 00 54 01 00 00 08 07 00 00 04 00 00 00 44 14 00 00 68 08 00 00 0e 00 00 00 24 00 00 00 ac 1c 00 00 05 00 00 00 e4 02 00 00 5c 3b 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 b0 23 00 00 8c 32 01 00 15 00 00 00 ec 01 00 00 d0 1c 00 00 16 00 00 00 98 00 00 00 bc 1e 00 00	....T.....D...h.....$.....\;.....`....8.....T.....#...2.....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 31 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.1.0.0.<./.P.i.d.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	68	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 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.a.m.p.l.e.4...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 37 00 30 00 31 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.>.8.7.0.1.8.<./.U.p.t.i.m.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 30 00 34 00 36 00 35 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.>.1.0.4.0.4.6.5.9.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 30 00 33 00 38 00 34 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.>.1.0.4.0.3.8.4.0.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 30 00 38 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.>.3.0.8.0.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 31 00 37 00 32 00 36 00 38 00 34 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.>.1.1.7.2.6.8.4.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 31 00 37 00 32 00 32 00 37 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.>.1.1.7.2.2.7.5.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 39 00 31 00 38 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 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.>.1.9.1.8.3.2.<./.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 39 00 31 00 36 00 30 00 38 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.>.1.9.1.6.0.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 33 00 36 00 34 00 34 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.>.3.6.4.4.8.<./.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 33 00 36 00 31 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.>.3.6.1.7.6.<./.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 32 00 34 00 36 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.>.2.4.6.1.6.9.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 32 00 34 00 36 00 39 00 38 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.>.2.4.6.9.8.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 32 00 34 00 36 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.>.2.4.6.1.6.9.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.3.8.8.<./.P.i.d.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 31 00 34 00 38 00 31 00 36 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.>.6.1.4.8.1.6.6.<./.U.p.t.i.m.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 37 00 33 00 34 00 32 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.>.5.7.3.4.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 35 00 33 00 34 00 35 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.>.1.0.5.3.4.5.0.2.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 34 00 30 00 36 00 37 00 30 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.>.1.0.4.0.6.7.0.7.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 37 00 37 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.>.9.7.7.6.8.8.<./.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	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 38 00 39 00 30 00 35 00 32 00 38 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.>.8.9.0.5.2.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 33 00 34 00 30 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.>.7.3.4.0.8.<./.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 37 00 38 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.>.6.8.7.8.4.<./.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 30 00 30 00 30 00 30 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.>.3.5.0.0.0.3.2.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 33 00 31 00 38 00 36 00 35 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.>.3.7.3.1.8.6.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 30 00 30 00 30 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.>.3.5.0.0.0.3.2.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 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.>.B.E.X.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 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.a.m.p.l.e.4...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 79 00 67 00 63 00 6f 00 70 00 78 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.>.y.g.c.o.p.x.,. .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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 79 00 67 00 63 00 6f 00 70 00 78 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.>.y.g.c.o.p.x.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 35 00 39 00 32 00 39 00 31 00 32 00 38 00 35 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.>.1.5.5.9.2.9.1.2.8.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 31 00 2d 00 31 00 34 00 54 00 31 00 32 00 3a 00 30 00 34 00 3a 00 31 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.-.0.1.-.1.4.T.1.2.:.0.4.:.1.4.Z.".>.	success or wait	1	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	266	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 33 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 31 00 30 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 37 00 33 00 30 00 34 00 36 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 37 00 33 00 30 00 34 00 36 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.3.9.". .P.I.D.=.".2.1.0.0.". .U.p.t.i.m.e.M.S.=.".7.3.0.4. 6.". .T.i.m.e.S.i.n.c.e.C.r.e. a.t.i.o.n.M.S.=.".7.3.0.4.6.". .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	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 62 00 37 00 37 00 65 00 65 00 33 00 36 00 2d 00 65 00 30 00 34 00 30 00 2d 00 34 00 35 00 61 00 66 00 2d 00 62 00 30 00 63 00 66 00 2d 00 34 00 32 00 66 00 35 00 33 00 63 00 64 00 31 00 33 00 33 00 31 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.7.b.7.7.e.e.3.6.-.e.0.4.0.-.4.5.a.f.-.b.0.c.f.-.4.2.f.5.3.c.d.1.3.3.1.6.<./.G.u.i.d.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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 31 00 2d 00 31 00 34 00 54 00 31 00 32 00 3a 00 30 00 34 00 3a 00 31 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.-.0.1.-.1.4.T.1.2.:.0.4.:.1.4.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD677.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	6E4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE76.tmp.xml	unknown	4753	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	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_177de25c\Report.wer	unknown	2	ff fe	..	success or wait	1	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_177de25c\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	174	6E4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_177de25c\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 35 00 30 00 34 00 31 00 35 00 36 00 36 00 36 00 36 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.5.0.4.1.5.6.6.6.6.	success or wait	1	6E4C497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{b2a94db5-e596-c614-1603-a508044e8fd9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{b2a94db5-e596-c614-1603-a508044e8fd9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E4E36BF	unknown
\REGISTRY\A\{b2a94db5-e596-c614-1603-a508044e8fd9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E4C43D1	unknown

Analysis Process: WerFault.exe PID: 620 Parent PID: 2100

General

Start time:	04:04:19
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2100 -s 896
Imagebase:	0x9e0000
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	6E421717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4DB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4DB.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_023208c1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_023208c1\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E41497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4DB.tmp	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4DB.tmp.xml	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER50B.tmp.csv	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FA.tmp.txt	success or wait	1	6E41497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 47 33 00 60 a4 05 12 00 00 00 00 00	MDMP..... .....G3.`.....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.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 1f 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 34 08 00 00 e6 32 00 60 3a 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 0d 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... ....4....2.`:................. ....0.................. 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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.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 89 6c 24 24 84 fa 9e 03 00 00 00 00 00 00 0d 00 89 6c 24 24 00 00 00 00 90 fa 9e 03 89 6c 24 24 23 00 00 00 46 02 01 00 74 fa 9e 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	....+...S...+. ..+....l$$.............l$$.... .....l$$#...F...t...+.........	success or wait	1	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	unknown	168	dc 0c 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 89 6c 24 24 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 89 6c 24 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 b2 25 00 00	.........................l$$.. ....l$$........ ....%..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	unknown	20	2a 00 00 00 54 f9 45 03 00 00 00 00 ac 06 00 00 82 41 00 00	*...T.E..........A..	success or wait	42	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	unknown	1708	bc b1 e5 77 d6 c9 e3 77 e8 02 00 00 aa aa aa aa 10 00 00 00 e8 f9 45 03 b4 fa 45 03 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa aa aa aa aa 00 00 00 00 78 6d 4a 01 e8 02 00 00 aa aa aa aa e8 02 00 00 aa aa aa aa aa aa aa aa 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 aa aa aa aa 28 51 49 01 00 00 00 00 00 00 00 00 50 8e 46 01 00 b0 10 01 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 68 fc 8e 03 44 fc 81 01 f0 2a 49 01 f0 2a 49 01 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	...w...w..............E...E... ..@..w@..w............xmJ..... ....(QI... ......P.F..................... ....h...D. ...*I..*I.....................	success or wait	41	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	unknown	1196	bc b1 e5 77 d6 c9 e3 77 b4 00 00 00 aa aa aa aa 10 00 00 00 e8 fb 71 01 b4 fc 71 01 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 d0 11 01 00 d0 11 01 00 00 00 00 b4 00 00 00 aa aa aa aa b4 00 00 00 aa aa aa aa 00 d0 11 01 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 aa aa aa aa f0 90 48 01 00 00 00 00 00 00 00 00 18 69 45 01 00 b0 10 01 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 44 fc 81 01 d4 fb 34 03 4c fc 81 01 88 6d 45 01 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	...w...w..............q...q... ..@..w@..w.................... ....H... ....iE..................... ....D..... 4.L....mE.....................	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	unknown	4	08 00 00 00	....	success or wait	8	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.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 68 03 00 00 00 00 00 00 e0 e1 49 01 00 00 00 00 00 00 00 00 00 00 00 00 04 f6 2f 01 2c 95 e5 77 23 00 00 00 02 02 00 00 94 f5 2f 01 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...+. ..+...h.........I............. ../.,..w#........./.+.........	success or wait	8	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	unknown	48	94 15 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 c0 12 01 00 00 00 00 94 f5 ae 03 00 00 00 00 6c 0a 00 00 e2 18 01 00 cc 02 00 00 12 3c 00 00	....l............<..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	unknown	4	31 00 00 00	1...	success or wait	49	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	unknown	28	16 00 00 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 00 2e 00 65 00 78 00 65 00 00 00	....s.a.m.p.l.e.4...e.x.e...	success or wait	49	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	unknown	120	00 00 1e 70 00 00 00 00 00 e0 08 00 80 b3 09 00 54 0a bf fd 5c 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 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 01 00 00 00	...p.....T...\%..... .....B.....B?..... .....#..... ..@A.....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.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	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	unknown	668	00 00 7e 73 00 00 00 00 00 10 01 00 03 ab 01 00 c4 1f 6d 8d 76 25 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 f0 f8 01 00 00 00 00 00 60 af 02 00 00 00 00 c7 67 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 5b 32 01 00 00 00 00 00 fc 5e 03 00 00 00 00 00 4f 78 02 00 00 00 00 00 94 9b 1b 00 00 00 00 00 ac 63 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 64 71 12 00 00 00 00 00 84 d9 4e 58 00 00 00 00 55 7d c1 23 00 00 00 00 67 81 c6 0e 00 00 00 00 30 31 19 01 00 00 00 00 62 bb 00 00 02 01 01 00 25 d5 05 00 88 7a 0b 00 ac 63 04 00 fb 7e 15 00 64 71 12 00 10 5f 3f 00 02 42 01 00 be 8f 18 00 00 00 00 00 1f 78 27 00 19 aa 04	..~s.....m.v%.....Zb ....` .....g.....[2.. .....^.....Ox.....c .....@.....dq.....NX.... U}.#....g.....01.....b..... ..%....z...c...~..dq..._?..B.. .....x'....	success or wait	1	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	unknown	14222	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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF661.tmp.dmp	unknown	120	03 00 00 00 84 01 00 00 08 07 00 00 04 00 00 00 b0 14 00 00 98 08 00 00 0e 00 00 00 24 00 00 00 48 1d 00 00 05 00 00 00 a4 02 00 00 de 3e 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 68 25 00 00 20 3a 01 00 15 00 00 00 ec 01 00 00 6c 1d 00 00 16 00 00 00 98 00 00 00 58 1f 00 00	.....$.....H.....>.....`....8.....T.....h%..:.....l.....X...	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 31 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.1.0.0.<./.P.i.d.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	68	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 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.a.m.p.l.e.4...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 38 00 30 00 39 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.>.9.8.0.9.6.<./.U.p.t.i.m.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 35 00 39 00 33 00 38 00 39 00 34 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.>.1.0.5.9.3.8.9.4.4.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 35 00 39 00 33 00 30 00 37 00 35 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.>.1.0.5.9.3.0.7.5.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 31 00 36 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.>.3.1.6.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 32 00 30 00 37 00 30 00 39 00 31 00 32 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.>.1.2.0.7.0.9.1.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 32 00 30 00 36 00 32 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.>.1.2.0.6.2.7.2.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 39 00 32 00 39 00 31 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 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.>.1.9.2.9.1.2.<./.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 39 00 32 00 37 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.>.1.9.2.7.4.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 34 00 34 00 33 00 37 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.>.4.4.3.7.6.<./.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 34 00 34 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.>.4.4.1.0.4.<./.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 32 00 36 00 34 00 36 00 30 00 31 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.>.2.6.4.6.0.1.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 32 00 36 00 35 00 34 00 32 00 30 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.>.2.6.5.4.2.0.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 32 00 36 00 34 00 36 00 30 00 31 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.>.2.6.4.6.0.1.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.3.8.8.<./.P.i.d.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 31 00 35 00 39 00 32 00 39 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.>.6.1.5.9.2.9.1.<./.U.p.t.i.m.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 38 00 38 00 35 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.>.5.8.8.5.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 35 00 33 00 34 00 35 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.>.1.0.5.3.4.5.0.2.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 34 00 30 00 35 00 34 00 37 00 38 00 34 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.>.1.0.4.0.5.4.7.8.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 37 00 37 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.>.9.7.7.6.8.8.<./.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	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 38 00 39 00 30 00 37 00 36 00 38 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.>.8.9.0.7.6.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 33 00 34 00 30 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.>.7.3.4.0.8.<./.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 37 00 38 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.>.6.8.7.8.4.<./.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 34 00 38 00 36 00 35 00 31 00 35 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.>.3.4.8.6.5.1.5.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 33 00 31 00 38 00 36 00 35 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.>.3.7.3.1.8.6.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 34 00 38 00 36 00 35 00 31 00 35 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.>.3.4.8.6.5.1.5.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 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.>.B.E.X.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 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.a.m.p.l.e.4...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 79 00 67 00 63 00 6f 00 70 00 78 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.>.y.g.c.o.p.x.,. .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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 79 00 67 00 63 00 6f 00 70 00 78 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.>.y.g.c.o.p.x.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 35 00 39 00 32 00 39 00 31 00 32 00 38 00 35 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.>.1.5.5.9.2.9.1.2.8.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 31 00 2d 00 31 00 34 00 54 00 31 00 32 00 3a 00 30 00 34 00 3a 00 32 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.-.0.1.-.1.4.T.1.2.:.0.4.:.2.4.Z.".>.	success or wait	1	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	266	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 33 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 31 00 30 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 37 00 33 00 30 00 34 00 36 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 37 00 33 00 30 00 34 00 36 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.3.9.". .P.I.D.=.".2.1.0.0.". .U.p.t.i.m.e.M.S.=.".7.3.0.4. 6.". .T.i.m.e.S.i.n.c.e.C.r.e. a.t.i.o.n.M.S.=.".7.3.0.4.6.". .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	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 66 00 35 00 30 00 31 00 37 00 31 00 65 00 2d 00 63 00 37 00 61 00 33 00 2d 00 34 00 36 00 62 00 61 00 2d 00 62 00 63 00 38 00 35 00 2d 00 32 00 32 00 61 00 38 00 66 00 37 00 36 00 62 00 62 00 66 00 32 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.6.f.5.0.1.7.1.e.-.c.7.a.3.-.4.6.b.a.-.b.c.8.5.-.2.2.a.8.f.7.6.b.b.f.2.8.<./.G.u.i.d.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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 31 00 2d 00 31 00 34 00 54 00 31 00 32 00 3a 00 30 00 34 00 3a 00 32 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.-.0.1.-.1.4.T.1.2.:.0.4.:.2.4.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD.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	6E41497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4DB.tmp.xml	unknown	4753	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	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_023208c1\Report.wer	unknown	2	ff fe	..	success or wait	1	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_023208c1\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	175	6E41497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_023208c1\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 35 00 31 00 30 00 30 00 39 00 30 00 32 00 37 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.7.5.1.0.0.9.0.2.7.	success or wait	1	6E41497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f4fcf9a2-270d-b1a9-2952-af6d939b3d1c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E4336BF	unknown
\REGISTRY\A\{f4fcf9a2-270d-b1a9-2952-af6d939b3d1c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E4336BF	unknown
\REGISTRY\A\{f4fcf9a2-270d-b1a9-2952-af6d939b3d1c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E4143D1	unknown

Analysis Process: WerFault.exe PID: 5008 Parent PID: 2100

General

Start time:	04:04:29
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2100 -s 924
Imagebase:	0x9e0000
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	6DEE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32EF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32EF.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_13ce361a	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_13ce361a\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32EF.tmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32EF.tmp.xml	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32F3.tmp.csv	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3575.tmp.txt	success or wait	1	6DED497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 53 33 00 60 a4 05 12 00 00 00 00 00	MDMP..... .....S3.`.....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.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 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 34 08 00 00 e6 32 00 60 3a 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 0d 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 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... ....4....2.`:................. ....0................. 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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.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 89 6c 24 24 1c f5 ae 03 00 00 00 00 00 00 0d 00 89 6c 24 24 00 00 00 00 28 f5 ae 03 89 6c 24 24 23 00 00 00 46 02 01 00 0c f5 ae 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	....+...S...+. ..+....l$$.............l$$.... (....l$$#...F.......+.........	success or wait	1	6DED497A	unknown

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	unknown	168	94 15 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 89 6c 24 24 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 89 6c 24 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 c8 26 00 00	........................l$$.. ....l$$........ ....&..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	unknown	20	2c 00 00 00 54 f9 45 03 00 00 00 00 ac 06 00 00 b8 42 00 00	,...T.E..........B..	success or wait	44	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	unknown	1708	bc b1 e5 77 d6 c9 e3 77 e8 02 00 00 aa aa aa aa 10 00 00 00 e8 f9 45 03 b4 fa 45 03 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa aa aa aa aa 00 00 00 00 78 6d 4a 01 e8 02 00 00 aa aa aa aa e8 02 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 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 aa aa aa aa 28 51 49 01 00 00 00 00 00 00 00 00 50 8e 46 01 00 b0 10 01 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 68 fc 8e 03 44 fc 81 01 00 fe 9e 03 f0 2a 49 01 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.............E...E... ..@..w@..w............xmJ..... ....(QI... ......P.F.................... ....h...D. ....*I....................	success or wait	43	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	unknown	1196	bc b1 e5 77 d6 c9 e3 77 b4 00 00 00 aa aa aa aa 10 00 00 00 e8 fb 71 01 b4 fc 71 01 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 d0 11 01 00 d0 11 01 00 00 00 00 b4 00 00 00 aa aa aa aa b4 00 00 00 aa aa aa aa 00 d0 11 01 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 aa aa aa aa f0 90 48 01 00 00 00 00 00 00 00 00 18 69 45 01 00 b0 10 01 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 44 fc 81 01 d4 fb 34 03 4c fc 81 01 88 6d 45 01 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	...w...w.............q...q... ..@..w@..w................... ....H... ....iE.................... ....D..... 4.L....mE....................	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	unknown	4	08 00 00 00	....	success or wait	8	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.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 68 03 00 00 00 00 00 00 e0 e1 49 01 00 00 00 00 00 00 00 00 00 00 00 00 04 f6 2f 01 2c 95 e5 77 23 00 00 00 02 02 00 00 94 f5 2f 01 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...+. ..+...h.........I............ ../.,..w#........./.+.........	success or wait	8	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	unknown	48	94 15 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 c0 12 01 00 00 00 00 2c e7 ae 03 00 00 00 00 d4 18 00 00 04 06 01 00 cc 02 00 00 28 3d 00 00	....,..... ....(=..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	unknown	4	33 00 00 00	3...	success or wait	51	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	unknown	28	16 00 00 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 00 2e 00 65 00 78 00 65 00 00 00	....s.a.m.p.l.e.4...e.x.e...	success or wait	51	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	unknown	120	00 00 94 70 00 00 00 00 00 30 01 00 80 1a 01 00 e7 ea 21 0c 6c 26 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 26 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 01 00 00 00	...p.....0.....!.l&..... .....B.....B?..... .....&..... ..@A.....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.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	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	unknown	668	00 00 7e 73 00 00 00 00 00 10 01 00 03 ab 01 00 c4 1f 6d 8d 8c 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 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 80 e8 01 00 00 00 00 00 60 af 02 00 00 00 00 02 6d 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 c2 36 01 00 00 00 00 00 fc 5e 03 00 00 00 00 00 4f 78 02 00 00 00 00 00 a9 a9 1b 00 00 00 00 00 97 55 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 64 71 12 00 00 00 00 00 80 1f 63 5c 00 00 00 00 d5 50 23 26 00 00 00 00 00 29 b2 2e 0f 00 00 00 00 00 85 51 2d 01 00 00 00 00 cd bf 00 00 14 19 01 00 af 10 06 00 87 85 0b 00 97 55 04 00 fb 7e 15 00 64 71 12 00 79 9a 42 00 4c 48 01 00 b6 04 1a 00 00 00 00 00 b4 66 29 00 3a ad 04	..~s.....m..&.....Zb ....m.....6.. .....^.....Ox.....U .....@.....dq.....c\.... .P#&....).....Q-..... .....U...~..dq..y.B.LH.. .....f).:..	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	unknown	14424	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 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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER286E.tmp.dmp	unknown	120	03 00 00 00 84 01 00 00 08 07 00 00 04 00 00 00 88 15 00 00 98 08 00 00 0e 00 00 00 24 00 00 00 20 1e 00 00 05 00 00 00 c4 02 00 00 f4 3f 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 e0 25 00 00 fc 35 01 00 15 00 00 00 ec 01 00 00 44 1e 00 00 16 00 00 00 98 00 00 00 30 20 00 00	.....$.....?.....`.....8.....T.....%...5.....D.....0 ..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 31 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.1.0.0.<./.P.i.d.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	68	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 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.a.m.p.l.e.4...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	46	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 30 00 30 00 30 00 30 00 33 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.>.1.1.0.0.0.3.<./.U.p.t.i.m.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 30 00 34 00 39 00 35 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.>.1.0.6.0.4.9.5.3.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 30 00 34 00 31 00 33 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.>.1.0.6.0.4.1.3.4.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 31 00 39 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.>.3.1.9.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 32 00 31 00 36 00 35 00 31 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.>.1.2.1.6.5.1.2.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 32 00 31 00 35 00 36 00 39 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.>.1.2.1.5.6.9.2.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 39 00 33 00 31 00 32 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.>.1.9.3.1.2.8.<./.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 39 00 32 00 39 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.>.1.9.2.9.6.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 35 00 31 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.>.5.1.4.0.0.<./.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 35 00 31 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.>.5.1.1.2.8.<./.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 32 00 36 00 38 00 36 00 39 00 37 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.>.2.6.8.6.9.7.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 32 00 36 00 39 00 35 00 31 00 36 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.>.2.6.9.5.1.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 32 00 36 00 38 00 36 00 39 00 37 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.>.2.6.8.6.9.7.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.3.8.8.<./.P.i.d.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 31 00 37 00 31 00 31 00 39 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.>.6.1.7.1.1.9.7.<./.U.p.t.i.m.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 39 00 30 00 30 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.>.5.9.0.0.0.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 35 00 33 00 34 00 35 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.>.1.0.5.3.4.5.0.2.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 39 00 36 00 37 00 35 00 35 00 37 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.>.9.6.7.5.5.7.1.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 37 00 37 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.>.9.7.7.6.8.8.<./.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	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 38 00 37 00 32 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.>.8.7.2.5.6.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 33 00 34 00 30 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.>.7.3.4.0.8.<./.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 37 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.>.6.7.2.8.8.<./.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 32 00 37 00 37 00 30 00 31 00 32 00 34 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.>.2.7.7.0.1.2.4.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 33 00 31 00 38 00 36 00 35 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.>.3.7.3.1.8.6.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 32 00 37 00 37 00 30 00 31 00 32 00 34 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.>.2.7.7.0.1.2.4.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 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.>.B.E.X.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 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.a.m.p.l.e.4...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 79 00 67 00 63 00 6f 00 70 00 78 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.>.y.g.c.o.p.x.,. .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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 79 00 67 00 63 00 6f 00 70 00 78 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.>.y.g.c.o.p.x.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 35 00 39 00 32 00 39 00 31 00 32 00 38 00 35 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.>.1.5.5.9.2.9.1.2.8.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 31 00 2d 00 31 00 34 00 54 00 31 00 32 00 3a 00 30 00 34 00 3a 00 33 00 36 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.-.0.1.-.1.4.T.1.2.:.0.4.:.3.6.Z.".>.	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	266	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 33 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 31 00 30 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 37 00 33 00 30 00 34 00 36 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 37 00 33 00 30 00 34 00 36 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.3.9.". .P.I.D.=.".2.1.0.0.". .U.p.t.i.m.e.M.S.=.".7.3.0.4. 6.". .T.i.m.e.S.i.n.c.e.C.r.e. a.t.i.o.n.M.S.=.".7.3.0.4.6.". .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	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 38 00 35 00 62 00 31 00 33 00 61 00 37 00 2d 00 31 00 30 00 33 00 63 00 2d 00 34 00 63 00 35 00 61 00 2d 00 62 00 62 00 33 00 35 00 2d 00 38 00 65 00 65 00 64 00 36 00 35 00 36 00 37 00 38 00 31 00 63 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.b.8.5.b.1.3.a.7.-.1.0.3.c.-.4.c.5.a.-.b.b.3.5.-.8.e.e.d.6.5.6.7.8.1.c.3.<./.G.u.i.d.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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 31 00 2d 00 31 00 34 00 54 00 31 00 32 00 3a 00 30 00 34 00 3a 00 33 00 36 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.-.0.1.-.1.4.T.1.2.:.0.4.:.3.6.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER306E.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	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32EF.tmp.xml	unknown	4753	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_13ce361a\Report.wer	unknown	2	ff fe	..	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_13ce361a\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	177	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_13ce361a\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 32 00 39 00 37 00 39 00 32 00 31 00 32 00 38 00 35 00	M.e.t.a.d.a.t.a.H.a.s.h.=.2.9.7.9.2.1.2.8.5.	success or wait	1	6DED497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a2c7132c-32a6-fad0-a764-545212197ff6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DEF36BF	unknown
\REGISTRY\A\{a2c7132c-32a6-fad0-a764-545212197ff6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DEF36BF	unknown
\REGISTRY\A\{a2c7132c-32a6-fad0-a764-545212197ff6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DED43D1	unknown

Analysis Process: WerFault.exe PID: 5764 Parent PID: 2100

General

Start time:	04:04:40
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2100 -s 1224
Imagebase:	0x9e0000
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	6E331717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER585A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER585A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_16da5cdc	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_16da5cdc\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E32497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER585A.tmp	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER585A.tmp.xml	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER586F.tmp.csv	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BCC.tmp.txt	success or wait	1	6E32497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 5d 33 00 60 a4 05 12 00 00 00 00 00	MDMP..... .....]3.`.....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.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 24 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 34 08 00 00 e6 32 00 60 3a 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 0d 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... ....4....2.`:................. ....0.................. 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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.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 89 6c 24 24 14 fb be 03 00 00 00 00 00 00 0d 00 89 6c 24 24 00 00 00 00 20 fb be 03 89 6c 24 24 23 00 00 00 46 02 01 00 04 fb be 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	....+...S...+. ..+....l$$.............l$$.... ....l$$#...F.......+.........	success or wait	1	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	unknown	168	40 16 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 89 6c 24 24 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 89 6c 24 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 d0 2b 00 00	@........................l$$.. ....l$$........ ....+..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	unknown	20	37 00 00 00 54 f9 45 03 00 00 00 00 ac 06 00 00 3c 4b 00 00	7...T.E.........<K..	success or wait	55	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	unknown	1708	bc b1 e5 77 d6 c9 e3 77 e8 02 00 00 aa aa aa aa 10 00 00 00 e8 f9 45 03 b4 fa 45 03 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa aa aa aa aa 00 00 00 00 60 2b 49 01 e8 02 00 00 aa aa aa aa e8 02 00 00 aa aa aa aa aa aa aa aa 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 aa aa aa aa 28 51 49 01 00 00 00 00 00 00 00 00 60 52 4a 01 00 b0 10 01 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 68 fc 8e 03 44 fc 81 01 00 fe 9e 03 f0 2a 49 01 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	...w...w..............E...E... ..@..w@..w............`+I..... .............................. .............................. ........................(QI... ......`RJ..................... ....h...D. ....*I.....................	success or wait	54	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	unknown	1196	bc b1 e5 77 d6 c9 e3 77 b4 00 00 00 aa aa aa aa 10 00 00 00 e8 fb 71 01 b4 fc 71 01 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 d0 11 01 00 d0 11 01 00 00 00 00 b4 00 00 00 aa aa aa aa b4 00 00 00 aa aa aa aa 00 d0 11 01 00 00 00 00 00 00 00 00 00 00 00 00 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 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa f0 90 48 01 00 00 00 00 00 00 00 00 18 69 45 01 00 b0 10 01 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 44 fc 81 01 d4 fb 34 03 4c fc 81 01 88 6d 45 01 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.............q...q... ..@..w@..w................... ....H... ....iE..................... ....D..... 4.L....mE.....................	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	unknown	4	09 00 00 00	....	success or wait	9	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.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 48 e2 2f 01 2c 95 e5 77 23 00 00 00 06 02 00 00 28 e2 2f 01 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#.......(./.+.........	success or wait	9	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	unknown	48	40 16 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 f0 12 01 00 00 00 00 24 ed be 03 00 00 00 00 dc 12 00 00 dc 54 00 00 cc 02 00 00 fc 44 00 00	@....... ....$..... .......T.......D..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	unknown	4	3c 00 00 00	<...	success or wait	60	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	unknown	28	16 00 00 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 00 2e 00 65 00 78 00 65 00 00 00	....s.a.m.p.l.e.4...e.x.e...	success or wait	60	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	unknown	120	00 00 ae 6f 00 00 00 00 00 b0 01 00 9c 87 02 00 e5 2a d0 19 72 2b 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 00 0c 00 00 00 18 00 00 00 01 00 00 00	...o.....*..r+.....B.....B?.....'.....A.....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.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	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	unknown	668	00 00 7e 73 00 00 00 00 00 10 01 00 03 ab 01 00 c4 1f 6d 8d 94 2b 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 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 80 f5 01 00 00 00 00 00 60 af 02 00 00 00 00 20 6e 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 a8 33 01 00 00 00 00 00 fc 5e 03 00 00 00 00 00 4f 78 02 00 00 00 00 00 ea 94 1b 00 00 00 00 00 56 6a 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 64 71 12 00 00 00 00 00 22 30 a6 61 00 00 00 00 a8 a1 34 28 00 00 00 00 ac 90 69 0f 00 00 00 00 a2 b8 42 01 00 00 00 00 48 c2 00 00 81 30 01 00 c1 50 06 00 fa 71 0b 00 56 6a 04 00 fb 7e 15 00 64 71 12 00 71 0f 45 00 60 4e 01 00 6c 5e 1b 00 00 00 00 00 d3 a8 2a 00 c0 ae 04	..~s.....m..+.....Zb.....`.....n.....3.....^.....Ox.....Vj.....@.....dq....."0.a....4(.....i.....B.....H....0...P...q..Vj...~..dq..q.E.`N..l^.....*....	success or wait	1	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	unknown	19742	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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4983.tmp.dmp	unknown	120	03 00 00 00 b4 01 00 00 08 07 00 00 04 00 00 00 54 19 00 00 c8 08 00 00 0e 00 00 00 24 00 00 00 1c 22 00 00 05 00 00 00 74 03 00 00 c8 47 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 c0 31 00 00 ba 53 01 00 15 00 00 00 ec 01 00 00 40 22 00 00 16 00 00 00 98 00 00 00 2c 24 00 00	.....T.....$.....".....t....G.....`....8.....T.....1...S.....@".....,$..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 31 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.1.0.0.<./.P.i.d.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	68	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 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.a.m.p.l.e.4...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	46	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 39 00 36 00 32 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.>.1.1.9.6.2.8.<./.U.p.t.i.m.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 31 00 30 00 34 00 36 00 30 00 39 00 32 00 38 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.>.1.1.0.4.6.0.9.2.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 31 00 30 00 34 00 35 00 32 00 37 00 33 00 36 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.>.1.1.0.4.5.2.7.3.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 35 00 37 00 39 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.>.3.5.7.9.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 35 00 37 00 34 00 31 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.>.1.3.5.7.4.1.4.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 35 00 36 00 35 00 39 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.>.1.3.5.6.5.9.5.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 39 00 37 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.>.2.0.9.7.0.4.<./.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 39 00 35 00 32 00 38 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.>.2.0.9.5.2.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 34 00 39 00 31 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.>.6.4.9.1.2.<./.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 34 00 36 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.>.6.4.6.4.0.<./.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 33 00 30 00 34 00 37 00 34 00 32 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.>.3.0.4.7.4.2.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 33 00 30 00 35 00 39 00 37 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.>.3.0.5.9.7.1.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 33 00 30 00 34 00 37 00 34 00 32 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.>.3.0.4.7.4.2.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.3.8.8.<./.P.i.d.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 31 00 38 00 30 00 37 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.>.6.1.8.0.7.7.5.<./.U.p.t.i.m.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 36 00 30 00 34 00 37 00 35 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.>.6.0.4.7.5.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 35 00 33 00 34 00 35 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.>.1.0.5.3.4.5.0.2.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 32 00 32 00 31 00 39 00 37 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.>.1.0.2.2.1.9.7.7.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 37 00 37 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.>.9.7.7.6.8.8.<./.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	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 38 00 37 00 32 00 37 00 38 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.>.8.7.2.7.8.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 33 00 34 00 30 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.>.7.3.4.0.8.<./.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 37 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.>.6.7.6.9.6.<./.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 33 00 35 00 37 00 30 00 38 00 31 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.>.3.3.5.7.0.8.1.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 33 00 31 00 38 00 36 00 35 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.>.3.7.3.1.8.6.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 33 00 35 00 37 00 30 00 38 00 31 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.>.3.3.5.7.0.8.1.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 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.>.B.E.X.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 73 00 61 00 6d 00 70 00 6c 00 65 00 34 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.a.m.p.l.e.4...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 79 00 67 00 63 00 6f 00 70 00 78 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.>.y.g.c.o.p.x.,. .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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 79 00 67 00 63 00 6f 00 70 00 78 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.>.y.g.c.o.p.x.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 35 00 39 00 32 00 39 00 31 00 32 00 38 00 35 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.>.1.5.5.9.2.9.1.2.8.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 31 00 2d 00 31 00 34 00 54 00 31 00 32 00 3a 00 30 00 34 00 3a 00 34 00 36 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.-.0.1.-.1.4.T.1.2.:.0.4.:.4.6.Z.".>.	success or wait	1	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	266	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 33 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 31 00 30 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 37 00 33 00 30 00 34 00 36 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 37 00 33 00 30 00 34 00 36 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.3.9.". .P.I.D.=.".2.1.0.0.". .U.p.t.i.m.e.M.S.=.".7.3.0.4. 6.". .T.i.m.e.S.i.n.c.e.C.r.e. a.t.i.o.n.M.S.=.".7.3.0.4.6.". .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	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 66 00 36 00 38 00 34 00 62 00 31 00 66 00 2d 00 62 00 35 00 61 00 61 00 2d 00 34 00 30 00 35 00 64 00 2d 00 61 00 63 00 62 00 62 00 2d 00 38 00 61 00 64 00 39 00 63 00 36 00 63 00 34 00 66 00 31 00 65 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.0.f.6.8.4.b.1.f.-.b.5.a.a.-.4.0.5.d.-.a.c.b.b.-.8.a.d.9.c.6.c.4.f.1.e.1.<./.G.u.i.d.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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 31 00 2d 00 31 00 34 00 54 00 31 00 32 00 3a 00 30 00 34 00 3a 00 34 00 36 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.-.0.1.-.1.4.T.1.2.:.0.4.:.4.6.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55D8.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	6E32497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER585A.tmp.xml	unknown	4753	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	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_16da5cdc\Report.wer	unknown	2	ff fe	..	success or wait	1	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_16da5cdc\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	186	6E32497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_sample4.exe_45365feab801c9585ad9627648598a0b3f59_b2de38ec_16da5cdc\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 33 00 31 00 37 00 30 00 38 00 39 00 32 00 31 00 36 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.3.1.7.0.8.9.2.1.6.	success or wait	1	6E32497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5ff033ba-dc3e-d921-483b-3b18e216edae}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E3436BF	unknown
\REGISTRY\A\{5ff033ba-dc3e-d921-483b-3b18e216edae}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E3436BF	unknown
\REGISTRY\A\{5ff033ba-dc3e-d921-483b-3b18e216edae}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E3243D1	unknown

Disassembly

Code Analysis