ID: 324174
Sample Name: KeJ7Cl7flZ.exe
Cookbook: default.jbs
Time: 15:04:21
Date: 28/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

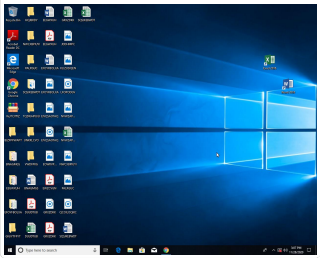
Analysis Report KeJ7Cl7flZ.exe

Overview

General Information

Sample Name:	KeJ7Cl7flZ.exe
Analysis ID:	324174
MD5:	4e759849412063..
SHA1:	40d132516cc4b9..
SHA256:	7a79f0c95e891b9.
Tags:	ArkeiStealer exe

Most interesting Screenshot:



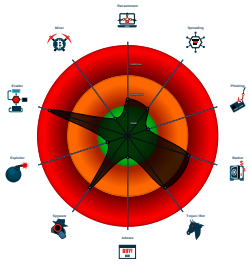
Detection

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

Signatures

- Antivirus detection for dropped file
- Detected unpacking (changes PE se…
- Detected unpacking (creates a PE fi…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Binary contains a suspicious time st…
- Contains functionality to check if a d…
- Contains functionality to detect slee…
- Contains functionality to infect the b…
- Drops PE files to the document folde…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- May check the online IP address of

Classification



Startup

- **System is w10x64**
- KeJ7Cl7flZ.exe (PID: 4576 cmdline: 'C:\Users\user\Desktop\KeJ7Cl7flZ.exe' MD5: 4E759849412063C6590936671CE4AA0E)
  - 002.exe (PID: 3568 cmdline: 'C:\Users\user\AppData\Local\Temp\RarSFX0\002.exe' MD5: 6503C9C4F19A4B33B701CC5B97B349BC)
    - WerFault.exe (PID: 204 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3568 -s 724 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 204 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3568 -s 740 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - Setup.exe (PID: 6668 cmdline: 'C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe' MD5: 62EAEA103DD9BEB69E884F2EDE1ACD63)
    - setup.exe (PID: 6732 cmdline: 'C:\Users\user\AppData\Local\Temp\sib309A.tmp\0\setup.exe' -s MD5: D64E3CC11AFC6331715BDFEC5F26C2A0)
      - aliens.exe (PID: 1112 cmdline: 'C:\Program Files (x86)\ujvqkl7ofji6\aliens.exe' MD5: 0F88FD9D557FFBE67A8897FB0FC08EE7)
  - jg2_2qua.exe (PID: 5292 cmdline: 'C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe' MD5: 676757904C8383FD9ACBEED15AA8DCC4)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.511085870.000000000331 0000.00000040.00000001.sdmp	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n

Unpacked PEs

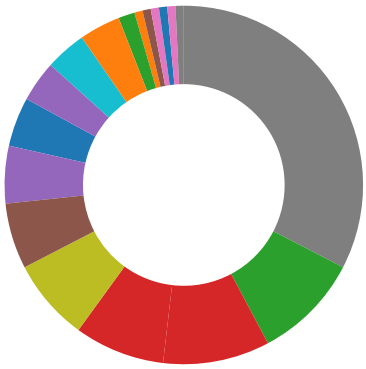
Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
19.2.aliens.exe.3310000.5.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
19.2.aliens.exe.10000000.6.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
19.2.aliens.exe.3310000.5.raw.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Protection of GUI
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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 detection for dropped file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

May check the online IP address of the machine

E-Banking Fraud:

Registers a new ROOT certificate

System Summary:

PE file has a writeable .text section

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (creates a PE file in dynamic memory)

Binary contains a suspicious time stamp

Persistence and Installation Behavior:

Contains functionality to infect the boot sector

Drops PE files to the document folder of the user

Boot Survival:

Contains functionality to infect the boot sector

Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

Stealing of Sensitive Information:

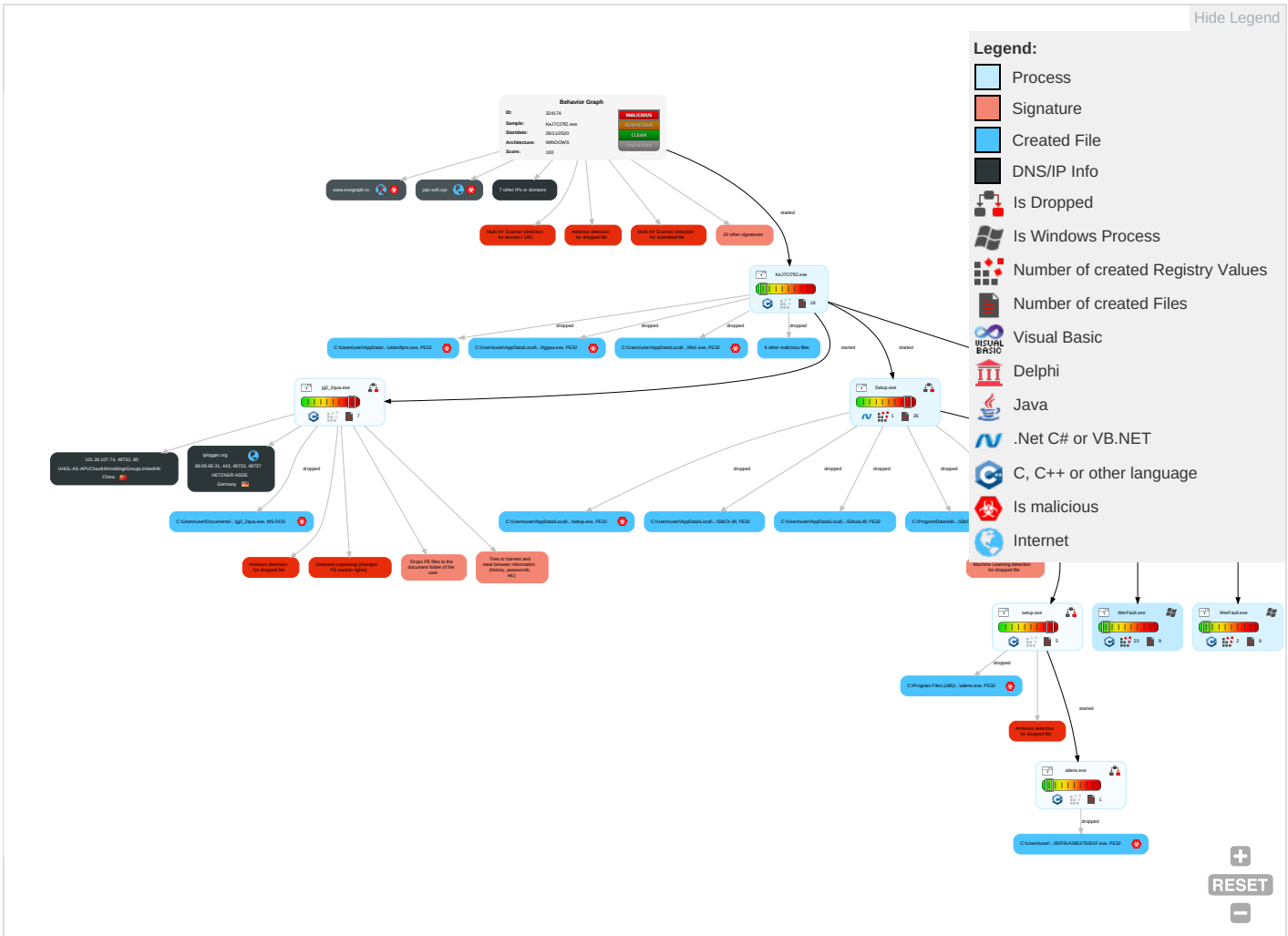
Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
Valid Accounts 2	Native API 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 2 1	OS Credential Dumping 1	System Time Discovery 1 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingre Trans
Default Accounts	Command and Scripting Interpreter 3	Application Shimming 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	Input Capture 3 1	File and Directory Discovery 4	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encry Chan
Domain Accounts	At (Linux)	Create Account 1	Application Shimming 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 5 7	SMB/Windows Admin Shares	Input Capture 3 1	Automated Exfiltration	Non-Appli Laye Proto
Local Accounts	At (Windows)	Valid Accounts 2	Valid Accounts 2	Install Root Certificate 1	NTDS	Query Registry 2	Distributed Component Object Model	Clipboard Data 2	Scheduled Transfer	Appli Laye Proto
Cloud Accounts	Cron	Bootkit 1	Access Token Manipulation 2 1	Software Packing 2 4	LSA Secrets	Security Software Discovery 2 7 1	SSH	Keylogging	Data Transfer Size Limits	Fallb Chan
Replication Through Removable Media	Launchd	Rc.common	Process Injection 1 2	Timestomp 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Process Discovery 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and (
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appli Laye
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Valid Accounts 2	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Modify Registry 1	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File T Proto
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Virtualization/Sandbox Evasion 4	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail I
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Access Token Manipulation 2 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Process Injection 1 2	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy
Trusted Relationship	Python	Hypervisor	Process Injection	Bootkit 1	Web Portal Capture	Cloud Groups	Attack PC via USB Connection	Local Email Collection	Standard Application Layer Protocol	Interr

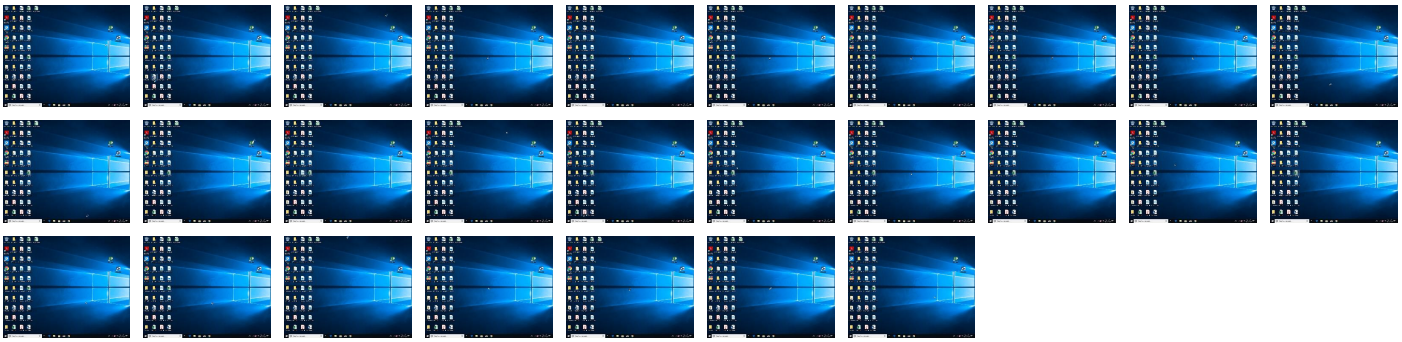
Behavior Graph



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
KeJ7CI7flZ.exe	67%	Virustotal		Browse
KeJ7CI7flZ.exe	79%	ReversingLabs	Win32.Downloader.Upatre	
KeJ7CI7flZ.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe	100%	Avira	HEUR/AGEN.1139239	
C:\Users\user\AppData\Local\Temp\sib309A.tmp\0\setup.exe	100%	Avira	TR/Siggen.lhhpy	
C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe	100%	Avira	TR/Crypt.CFI.Gen	
C:\Users\user\Documents\VlcpVideoV1.0.1\jg2_2qua.exe	100%	Avira	TR/Crypt.CFI.Gen	
C:\Users\user\AppData\Local\Temp\RarSFX0\hjjgaa.exe	100%	Avira	HEUR/AGEN.1134829	
C:\Users\user\AppData\Local\Temp\RarSFX0\002.exe	100%	Avira	TR/AD.PredatorThief.gldkk	
C:\Users\user\AppData\Local\Temp\RarSFX0\file1.exe	100%	Avira	TR/AD.JamkeeDldr.gwmgy	
C:\Users\user\AppData\Local\Temp\RarSFX0\ubisoftpro.exe	100%	Avira	TR/AD.ColtyStealer.mwfxd	
C:\Users\user\AppData\Local\Temp\RarSFX0\askinstall21.exe	100%	Avira	HEUR/AGEN.1138531	
C:\Users\user\AppData\Local\Temp\RarSFX0\BTRSetp.exe	100%	Avira	TR/Kryptik.ijozo	
C:\Users\user\AppData\Local\Temp\85F91A36E275562F.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe	100%	Joe Sandbox ML		
C:\Users\user\Documents\VlcpVideoV1.0.1\jg2_2qua.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RarSFX0\hjjgaa.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RarSFX0\002.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RarSFX0\file1.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RarSFX0\ubisoftpro.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RarSFX0\askinstall21.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RarSFX0\SSSS.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\ujvqkl7ofji6\aliens.exe	100%	Joe Sandbox ML		
C:\ProgramData\sib\{F9266136-0000-46F8-BC66-FDD9185E4296}\SibClr.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.2.Setup.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139321		Download File
19.2.aliens.exe.2f00000.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
26.0.jg2_2qua.exe.400000.0.unpack	100%	Avira	TR/Crypt.CFI.Gen		Download File
15.0.Setup.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139321		Download File
1.2.002.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
jojo-soft.xyz	9%	Virustotal		Browse
evograph.ro	7%	Virustotal		Browse
trueaerned.com	1%	Virustotal		Browse
7553014bd6a4211b.xyz	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://101.36.107.74/seemorebty/il.php?e=jg2_2qua	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://www.ipcode.pw/	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/COMODOTimeStampingCA_2.crl0r	0%	Avira URL Cloud	safe	
http://ffdownload.online/business/receiveConnection:	0%	Avira URL Cloud	safe	
http://103.91.21Facebook	0%	Avira URL Cloud	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	Avira URL Cloud	safe	
http://https://apreltech.com/SilentInstallBuilder/Doc/&t=event&ec=%s&ea=%s&el=_	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://https://www.airbnb.cn/account-settingstext/html	0%	Avira URL Cloud	safe	
http://www.ipcode.pw/0.0.0.0CNpathSOFTWARE	0%	Avira URL Cloud	safe	
http://crl.como	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0B	0%	Avira URL Cloud	safe	
http://7553014BD6A4211B.xyz/info/w	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSec	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://7553014BD6A4211B.xyz/ng	0%	Avira URL Cloud	safe	
http://7553014BD6A4211B.xyz/	0%	Avira URL Cloud	safe	
http://101.36.107.74/seemorebty/	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/COMODOTimeStampingCA_2.crt0#	0%	Avira URL Cloud	safe	
http://ocsp.pki.goog/GTSGIAG30	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://crl.pki.goog/GTSGIAG3.crl0	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://101.36.10https://www.instH	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.comoZ	0%	Avira URL Cloud	safe	
http://ffdownload.online/business/receive	0%	Avira URL Cloud	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://crl.comoU	0%	Avira URL Cloud	safe	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=5864849777998;gt	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://www.airbnb.cn/account-settings	0%	Avira URL Cloud	safe	
http://7553014BD6A4211B.xyz/L	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://7553014bd6a4211b.xyz/0	0%	Avira URL Cloud	safe	
http://cookies.onetrust.mgr.consensu.org/onetrust-logo.svg	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSec)	0%	Avira URL Cloud	safe	
http://www.zxfc.pw/Home/Index/sksxz?uid=3a1c3033bf5a5764882caec7a4cf3849e7de2ef2a8d79cece23467f1d887	0%	Avira URL Cloud	safe	
http://www.fddnice.pw/	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://Ojyehq4jg.2ihsfa.com/	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
jojo-soft.xyz	104.31.72.130	true	true	• 9%, Virustotal, Browse	unknown
iplogger.org	88.99.66.31	true	false		high
ip-api.com	208.95.112.1	true	false		high
evograph.ro	89.40.17.17	true	false	• 7%, Virustotal, Browse	unknown
trueaerned.com	198.98.57.54	true	false	• 1%, Virustotal, Browse	unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
7553014bd6a4211b.xyz	172.67.157.133	true	false	• 5%, Virustotal, Browse	unknown
p421ls.xyz	104.31.90.245	true	false		unknown
g.msn.com	unknown	unknown	false		high
www.evograph.ro	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://101.36.107.74/seemorebty/il.php?e=jg2_2qua	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msn.com/de-ch/entertainment/_h/c920645c/webcore/externalscripts/oneTrustV2/scripttemplate	jg2_2qua.exe, 0000001A.00000003.489902919.0000000003E08000.00000004.00000001.sdmp	false		high
http://https://iplogger.org/1KyTy7	askinstall21.exe	false		high
http://ocsp.sectigo.com0	Setup.exe, 0000000F.00000002.467933755.0000000000420000.00000004.00020000.sdmp, jg2_2qua.exe, 0000001A.00000002.506529883.000000000071B000.00000004.00000020.sdmp, SibClr.dll.15.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=58648497779	jg2_2qua.exe, 0000001A.00000003.492557880.0000000003E20000.00000004.00000001.sdmp	false		high
http://www.ipcode.pw/	askinstall21.exe	false	• Avira URL Cloud: safe	unknown
http://crl.sectigo.com/COMODOTimeStampingCA_2.crl0r	hjjgaa.exe	false	• Avira URL Cloud: safe	unknown
http://ffdownload.online/business/receiveConnection:	002.exe	false	• Avira URL Cloud: safe	unknown
http://103.91.21Facebook	ubisoftpro.exe	false	• Avira URL Cloud: safe	low
http://https://deff.nelreports.net/api/report?cat=msn	jg2_2qua.exe, 0000001A.00000003.489902919.0000000003E08000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://apreltech.com/SilentInstallBuilder/Doc/&t=event&ec=%s&ea=%s&el=_	Setup.exe, 0000000F.00000002.476631772.000000006FF05000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.org/1XJq97	askinstall21.exe	false		high
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	Setup.exe, 0000000F.00000002.467933755.0000000000420000.00000004.00020000.sdmp, SibClr.dll.15.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.airbnb.cn/account-settingstext/html	ubisoftpro.exe	false	• Avira URL Cloud: safe	unknown
http://www.ipcode.pw/0.0.0.0CNpathSOFTWARE	askinstall21.exe	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.org/1T79i7	askinstall21.exe	false		high
http://crl.como	jg2_2qua.exe, 0000001A.00000003.481303695.0000000000726000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.org/1Uts87	askinstall21.exe	false		high
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e	jg2_2qua.exe, 0000001A.00000003.492557880.0000000003E20000.00000004.00000001.sdmp	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=3931852	jg2_2qua.exe, 0000001A.00000003.492557880.0000000003E20000.00000004.00000001.sdmp	false		high
http://charlesproxy.com/ssl	aliens.exe, 00000013.00000002.508576720.0000000000BB7000.00000004.00000020.sdmp, aliens.exe, 00000013.00000002.508666439.0000000000BCF000.00000004.00000020.sdmp	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	85F91A36E275562F.exe.19.dr	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	jg2_2qua.exe, 0000001A.00000003.492557880.0000000003E20000.00000004.00000001.sdmp	false		high
http://https://iplogger.org/1OhAG	askinstall21.exe	false		high
http://https://iplogger.org/1uVkt7	askinstall21.exe	false		high
http://https://sectigo.com/CPS0B	hjjgaa.exe	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/?ocid=iehp	jg2_2qua.exe, 0000001A.00000003.492557880.0000000003E20000.00000004.00000001.sdmp	false		high
http://https://iplogger.org/1b4887	askinstall21.exe	false		high
http://7553014BD6A4211B.xyz/info/w	aliens.exe, 00000013.00000002.508492865.0000000000B96000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSec	jg2_2qua.exe, 0000001A.00000002.506529883.000000000071B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.org/1OZVH	askinstall21.exe	false		high
http://https://sectigo.com/CPS0D	Setup.exe, 0000000F.00000002.467933755.0000000000420000.00000004.00020000.sdmp, SibClr.dll.15.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://iplogger.org/1UpU57	askinstall21.exe	false		high
http://7553014BD6A4211B.xyz/ng	aliens.exe, 00000013.00000002.508446733.0000000000B6A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.org/1O2BH	askinstall21.exe	false		high
http://https://iplogger.org/1XKq97	askinstall21.exe	false		high
http://https://iplogger.org/1TT4a7	John_Ship.url	false		high
http://https://iplogger.org/1XSq97	askinstall21.exe	false		high
http://7553014BD6A4211B.xyz/	aliens.exe, 00000013.00000002.508446733.0000000000B6A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://101.36.107.74/seemorebty/	jg2_2qua.exe, 0000001A.00000002.504458828.00000000004F4000.00000040.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/COMODOTimeStampingCA_2.crt0#	hjjgaa.exe	false	• Avira URL Cloud: safe	unknown
http://ocsp.pki.goog/GTSGIAG30	jg2_2qua.exe, 0000001A.00000003.495023797.0000000003E31000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://charlesproxy.com/ssl1	aliens.exe, 00000013.00000002.508576720.0000000000BB7000.00000004.00000020.sdmp	false		high
http://https://iplogger.org/19iM77	askinstall21.exe	false		high
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	jg2_2qua.exe, 0000001A.00000002.506529883.000000000071B000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://iplogger.org/1T89i7	askinstall21.exe	false		high
http://https://iplogger.org/16ajh7	askinstall21.exe	false		high
http://https://iplogger.org/2WS9q6ubisoftplushttps://iplogger.org/2WF9q6ubisoftsmphttps://iplogger.org/2WJ9	ubisoftpro.exe	false		high
http://https://sectigo.com/CPS0	Setup.exe, 0000000F.00000002.467933755.0000000000420000.00000004.00020000.sdmp, jg2_2qua.exe, 0000001A.00000002.506529883.000000000071B000.00000004.00000020.sdmp, SibClr.dll.15.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ip-api.com/json/countryCodecountry_codemac%s.exeSoftware	hjjgaa.exe	false		high
http://crl.pki.goog/GTSGIAG3.crl0	jg2_2qua.exe, 0000001A.00000003.495023797.0000000003E31000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.org/16xjh7	askinstall21.exe	false		high
http://ocsp.thawte.com0	85F91A36E275562F.exe.19.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://optanon.blob.core.windows.net/skins/4.1.0/default_flat_top_two_button_black/v2/css/optanon.c	jg2_2qua.exe, 0000001A.00000003.493765388.0000000003F30000.00000004.00000001.sdmp	false		high
http://https://iplogger.org/1X8M97	askinstall21.exe	false		high
http://https://iplogger.org/2WX9q6ubisoftmorehttps://iplogger.org/2WN9q6ubisoftablehttps://iplogger.org/2W6	ubisoftpro.exe	false		high
http://https://iplogger.org/ZdnY7	jg2_2qua.exe, 0000001A.00000003.480992334.000000000071B000.00000004.00000001.sdmp, jg2_2qua.exe, 0000001A.00000003.480069462.0000000000724000.00000004.00000001.sdmp	false		high
http://101.36.10https://www.instH	jg2_2qua.exe, 0000001A.00000002.503990767.0000000000401000.00000040.00020000.sdmp	false	• Avira URL Cloud: safe	low
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1	jg2_2qua.exe, 0000001A.00000003.492557880.0000000003E20000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	Setup.exe, 0000000F.00000002.467933755.0000000000420000.00000004.00020000.sdmp, SibClr.dll.15.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.comoZ	jg2_2qua.exe, 0000001A.00000002.506529883.000000000071B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://iplogger.org/1TW3i7	askinstall21.exe	false		high
http://https://iplogger.org/1q6Jt7	askinstall21.exe	false		high
http://7553014bd6a4211b.xyz/info/w	aliens.exe, 00000013.00000002.508492865.0000000000B96000.00000004.00000020.sdmp, aliens.exe, 00000013.00000002.508446733.0000000000B6A000.00000004.00000020.sdmp	false		unknown
http://ffdownload.online/business/receive	002.exe	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	Setup.exe, 0000000F.00000000.288312686.0000000000409000.00000002.00020000.sdmp, Setup.exe.0.dr	false		high
http://https://contextual.media.net/	jg2_2qua.exe, 0000001A.00000003.502245420.0000000004088000.00000004.00000001.sdmp	false		high
http://ocsp.pki.goog/gsr202	jg2_2qua.exe, 0000001A.00000003.495023797.0000000003E31000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://optanon.blob.core.windows.net/skins/4.1.0/default_flat_top_two_button_black/v2/images/cookie	jg2_2qua.exe, 0000001A.00000003.493765388.0000000003F30000.00000004.00000001.sdmp	false		high
http://https://pki.goog/repository/0	jg2_2qua.exe, 0000001A.00000003.495023797.0000000003E31000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.comoU	jg2_2qua.exe, 0000001A.00000003.480992334.000000000071B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=5864849777998;gt	jg2_2qua.exe, 0000001A.00000003.492557880.0000000003E20000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.org/1OXFG	askinstall21.exe	false		high
http://https://iplogger.org/1Ka7t7	askinstall21.exe	false		high
http://www.msn.com/	jg2_2qua.exe, 0000001A.00000003.502245420.0000000004088000.00000004.00000001.sdmp	false		high
http://https://iplogger.org/1bV787	askinstall21.exe	false		high
http://www.msn.com/de-ch/?ocid=iehp	jg2_2qua.exe, 0000001A.00000003.492557880.0000000003E20000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	Setup.exe, 0000000F.00000002.467933755.0000000000420000.00000004.00020000.sdmp, SibClr.dll.15.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=2542116;cat=chom0;ord=4842492154761;g	jg2_2qua.exe, 0000001A.00000003.492557880.0000000003E20000.00000004.00000001.sdmp	false		high
http://https://iplogger.org/1lC5g	askinstall21.exe	false		high
http://https://www.airbnb.cn/account-settings	ubisoftpro.exe	false	• Avira URL Cloud: safe	unknown
http://7553014BD6A4211B.xyz/L	aliens.exe, 00000013.00000002.508446733.0000000000B6A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	Setup.exe, 0000000F.00000002.467933755.0000000000420000.00000004.00020000.sdmp, SibClr.dll.15.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://7553014bd6a4211b.xyz/0	aliens.exe, 00000013.00000002.508446733.0000000000B6A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1	jg2_2qua.exe, 0000001A.00000003.492557880.0000000003E20000.00000004.00000001.sdmp	false		high
http://cookies.onetrust.mgr.consensu.org/onetrust-logo.svg	jg2_2qua.exe, 0000001A.00000003.493765388.0000000003F30000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSec)	jg2_2qua.exe, 0000001A.00000002.506529883.000000000071B000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.winimage.com/zLibDll	ubisoftpro.exe	false		high
http://www.zxfc.pw/Home/Index/sksxz?uid=3a1c3033bf5a5764882caec7a4cf3849e7de2ef2a8d79cece23467f1d887	askinstall21.exe	false	• Avira URL Cloud: safe	unknown
http://www.fddnice.pw/	askinstall21.exe	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	jg2_2qua.exe, 0000001A.00000003.495023797.0000000003E31000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://Ojyehq4jg.2ihsfa.com/	hjjgaa.exe	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTSGIAG3.crt0)	jg2_2qua.exe, 0000001A.00000003.495023797.0000000003E31000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://iplogger.org/1yXwr7	askinstall21.exe	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
101.36.107.74	unknown	China		135377	UHGL-AS-APUCloudHKHoldingsGroup LimitedHK	false
88.99.66.31	unknown	Germany		24940	HETZNER-ASDE	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324174
Start date:	28.11.2020
Start time:	15:04:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KeJ7Cl7flZ.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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winEXE@13/35@12/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.4% (good quality ratio 17.5%) • Quality average: 78.6% • Quality standard deviation: 28%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 92.122.144.200, 51.104.144.132, 20.54.26.129, 51.103.5.159, 52.142.114.176, 92.122.213.194, 92.122.213.247, 51.11.168.160, 104.43.139.144 • Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, ris.api.iris.microsoft.com, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found. • Too many dropped files, some of them have not been restored

Simulations

Behavior and APIs

Time	Type	Description
15:05:24	API Interceptor	2x Sleep call for process: WerFault.exe modified
15:07:10	API Interceptor	1x Sleep call for process: jg2_2qua.exe modified
15:07:41	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Windows Host C:\ProgramData\Windows Host\Windows Host.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
88.99.66.31	cli.exe	Get hash	malicious	Browse	• ezstat.ru /1BiQt7.html
	R7w74RKW9A.exe	Get hash	malicious	Browse	• ezstat.ru /1BiQt7.html
	pqSZtQiuRy.exe	Get hash	malicious	Browse	• iplogger. org/14mvt7.gz
	3MndTUzGQn.exe	Get hash	malicious	Browse	• iplogger. org/14qK87
	fEBNeNkRYI.doc	Get hash	malicious	Browse	• iplogger. org/1cyy87.jpg
	Delivery-77426522.doc	Get hash	malicious	Browse	• iplogger. org/1cyy87.jpg
	mesager43.exe	Get hash	malicious	Browse	• iplogger. org/1cyy87.jpg
	hci0xn0zip.exe	Get hash	malicious	Browse	• iplogger. org/1cyy87.jpg
	DOC001.exe	Get hash	malicious	Browse	• 2no.co/1Lan77
	DOC001 (3).exe	Get hash	malicious	Browse	• 2no.co/1Lan77
	urgently.exe	Get hash	malicious	Browse	• iplogger. org/1Uu547.tgz
	SecuriteInfo.com.Generic.mg.e26982b170856ca8.exe	Get hash	malicious	Browse	• iplogger. org/1Uu547.tgz
	trwf3446.doc	Get hash	malicious	Browse	• iplogger. org/1Uu547.tgz
	2020_1549496734.doc	Get hash	malicious	Browse	• maper.inf o/XtDei
	2020_1549496734.doc	Get hash	malicious	Browse	• maper.inf o/XtDei
	http://maper.info	Get hash	malicious	Browse	• maper.info/
	clipp.exe	Get hash	malicious	Browse	• iplogger. com/1NAnw7
	por.exe	Get hash	malicious	Browse	• ezstat.ru /1kDj27
	morfer.exe	Get hash	malicious	Browse	• iplo.ru/1 VJfB6.jpeg
	image2017-11-22-5864621.vbs	Get hash	malicious	Browse	• iplogger. co/18RtV6.jpg

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
iplogger.org	XC65ED9or6.exe	Get hash	malicious	Browse	• 88.99.66.31
	cli.exe	Get hash	malicious	Browse	• 88.99.66.31
	R7w74RKW9A.exe	Get hash	malicious	Browse	• 88.99.66.31
	pqSZtQiuRy.exe	Get hash	malicious	Browse	• 88.99.66.31
	a3d224d6da883da2d8ba5671ab64ed24.exe	Get hash	malicious	Browse	• 88.99.66.31
	a3d224d6da883da2d8ba5671ab64ed24.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.ArtemisE8B534F89B0F.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.PWS.Siggen2.59718.4609.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.PWS.Siggen2.59485.31175.exe	Get hash	malicious	Browse	• 88.99.66.31
	2rYTU7Mzo9.exe	Get hash	malicious	Browse	• 88.99.66.31
	3MndTUzGQn.exe	Get hash	malicious	Browse	• 88.99.66.31
	fEBNeNkRYI.doc	Get hash	malicious	Browse	• 88.99.66.31
	Delivery-77426522.doc	Get hash	malicious	Browse	• 88.99.66.31
	mesager43.exe	Get hash	malicious	Browse	• 88.99.66.31
	hci0xn0zip.exe	Get hash	malicious	Browse	• 88.99.66.31
	mAGgYcXJQt.exe	Get hash	malicious	Browse	• 88.99.66.31
	mAGgYcXJQt.exe	Get hash	malicious	Browse	• 88.99.66.31
	BfzImZE7zo.exe	Get hash	malicious	Browse	• 88.99.66.31
	ub3hVgo06u.exe	Get hash	malicious	Browse	• 88.99.66.31
	taEYMQQA1C.exe	Get hash	malicious	Browse	• 88.99.66.31
ip-api.com	ySlUZAKoMh.exe	Get hash	malicious	Browse	• 208.95.112.1
	si7zDzLSfK.exe	Get hash	malicious	Browse	• 208.95.112.1
	82XVDE9IWo.exe	Get hash	malicious	Browse	• 208.95.112.1

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	jFqDHL8zPX.exe	Get hash	malicious	Browse	• 208.95.112.1
	XC65ED9or6.exe	Get hash	malicious	Browse	• 208.95.112.1
	4jb976XCme.exe	Get hash	malicious	Browse	• 208.95.112.1
	4aU4qrHzwx.exe	Get hash	malicious	Browse	• 208.95.112.1
	2scEWJGJIQ.exe	Get hash	malicious	Browse	• 208.95.112.1
	R0BsJKRSF4.exe	Get hash	malicious	Browse	• 208.95.112.1
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	• 208.95.112.1
	Venom.exe	Get hash	malicious	Browse	• 208.95.112.1
	PO348578.jar	Get hash	malicious	Browse	• 208.95.112.1
	module.exe	Get hash	malicious	Browse	• 208.95.112.1
	Payment Swift.xlsx	Get hash	malicious	Browse	• 208.95.112.1
	WYkWMLlPvb.exe	Get hash	malicious	Browse	• 208.95.112.1
	WYkWMLlPvb.exe	Get hash	malicious	Browse	• 208.95.112.1
	SecuriteInfo.com.Trojan.GenericKDZ.71528.23323.exe	Get hash	malicious	Browse	• 208.95.112.1
	http://https://comvoce.philco.com.br/wp-forum/administracion/prelogin.php	Get hash	malicious	Browse	• 193.234.225.88
	TOOL.exe	Get hash	malicious	Browse	• 208.95.112.1
	pmL5ihWLvh.exe	Get hash	malicious	Browse	• 208.95.112.1
trueaerned.com	ySlUZAKoMh.exe	Get hash	malicious	Browse	• 198.98.57.54
	si7zDzLSfK.exe	Get hash	malicious	Browse	• 198.98.57.54
	4jb976XCme.exe	Get hash	malicious	Browse	• 198.98.57.54

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UHGL-AS-APUCloudHKHoldingsGroupLimitedHK	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 101.36.113.249
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 101.36.113.249
	DEWA PROJECT 12100317.exe	Get hash	malicious	Browse	• 101.36.113.249
	NP9K0ul0jfgmTjl.exe	Get hash	malicious	Browse	• 101.36.120.233
	Quotation.exe	Get hash	malicious	Browse	• 103.72.146.121
	Detalii 032411-959286.doc	Get hash	malicious	Browse	• 128.14.231.58
	Detalii 032411-959286.doc	Get hash	malicious	Browse	• 128.14.231.58
	Detalii 032411-959286.doc	Get hash	malicious	Browse	• 128.14.231.58
	http://phpyb.com/gmhtg/TZ/2Q/zNzgLzGa.zip	Get hash	malicious	Browse	• 152.32.211.197
HETZNER-ASDE	document-1475334804.xls	Get hash	malicious	Browse	• 78.46.235.88
	XC65ED9or6.exe	Get hash	malicious	Browse	• 88.99.66.31
	document-1475334804.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1471350090.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1471350090.xls	Get hash	malicious	Browse	• 78.46.235.88
	XcOxlmOz4D.exe	Get hash	malicious	Browse	• 95.217.228.176
	document-1482143404.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1482143404.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-15241477.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-15241477.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1528549920.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1528549920.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1523563474.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1523563474.xls	Get hash	malicious	Browse	• 78.46.235.88
	TaskAudio Driver.exe	Get hash	malicious	Browse	• 95.217.144.93
	document-1544626742.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1544626742.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1544163851.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1544163851.xls	Get hash	malicious	Browse	• 78.46.235.88
	coinomi-1.20.0.apk	Get hash	malicious	Browse	• 88.99.26.209

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	XC65ED9or6.exe	Get hash	malicious	Browse	• 88.99.66.31
	DHL invoice VNYI564714692.exe	Get hash	malicious	Browse	• 88.99.66.31
	Order-Poland.exe	Get hash	malicious	Browse	• 88.99.66.31
	Novi poredak.exe	Get hash	malicious	Browse	• 88.99.66.31
	Customer Remittance Advice 9876627262822662.exe	Get hash	malicious	Browse	• 88.99.66.31
	94039330.exe	Get hash	malicious	Browse	• 88.99.66.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	P1001094.EXE	Get hash	malicious	Browse	• 88.99.66.31
	New Order PO20011046.exe	Get hash	malicious	Browse	• 88.99.66.31
	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe	Get hash	malicious	Browse	• 88.99.66.31
	11-27.exe	Get hash	malicious	Browse	• 88.99.66.31
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 88.99.66.31
	caw.exe	Get hash	malicious	Browse	• 88.99.66.31
	6znqz0d1.dll	Get hash	malicious	Browse	• 88.99.66.31
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 88.99.66.31
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 88.99.66.31
	2zv940v7.dll	Get hash	malicious	Browse	• 88.99.66.31
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 88.99.66.31
	lzezma64.dll	Get hash	malicious	Browse	• 88.99.66.31
	fuxenm32.dll	Get hash	malicious	Browse	• 88.99.66.31
	api-cdef.dll	Get hash	malicious	Browse	• 88.99.66.31
37f463bf4616ecd445d4a1937da06e19	document-1456864371.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1365485901.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1363274030.xls	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Exploit.Siggen3.2597.23127.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1460962286.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1366355469.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1458916175.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1463039695.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1499051934.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1367992196.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1511069982.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1475334804.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1459095245.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1366980661.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1471350090.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1500752222.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1506903149.xls	Get hash	malicious	Browse	• 88.99.66.31
	http://culturenempathy.org/	Get hash	malicious	Browse	• 88.99.66.31
	case.8920.xls	Get hash	malicious	Browse	• 88.99.66.31
	document-1497815773.xls	Get hash	malicious	Browse	• 88.99.66.31

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\ujvqkl7ofji6\aliens.exe

Process:	C:\Users\user\AppData\Local\Temp\sib309A.tmp\0\setup.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	490274830
Entropy (8bit):	0.13399746942054178
Encrypted:	false
SSDEEP:	
MD5:	C4E00A325E324C12C52D45A2C5A0B7CA
SHA1:	F457B527850FB82A942A33DE7195356BA76F3C89
SHA-256:	A958A1908B2473BD3A7547122602ADF7FFAFC17D94B52E95CD99836CD1E6CE96
SHA-512:	301DC8DD9D61D90157D989CCC0F3D6897EC18EA6A6F3665D6647E6848C11C39D6A01D624914399CE5FAFA2914BEBAE830FB0C29D5B2A0C3BFD5D14693677F0 2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....3.!This program cannot be run in DOS mode....$.....-...i.i.i..9.k.`.:.w.`.,...`.+.P.N%.c.N%.H.i.d.`. ./.w.:.k.w.;.h.i.8.h.` .>.h.Richi.....PE..L.....K.....#.....@.....c..... ....@.....@.....@.....<...T.....P..... ....@.....text..... ....rdata..\.... .....@..@.data.....h.....@....rsrc...P.....H.....@..@..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_002.exe_1c529646ab3c8a1fdb7fc485aa1d9d3291c12_6234ae00_0086ee01\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12056
Entropy (8bit):	3.7759983087181124
Encrypted:	false
SSDEEP:	192:ylqpHMfd/UUT+njbttz/u7sUS274ItiRX:5qZMf1UUqjH/u7sUX4ItSX
MD5:	99CA516681EAE4643633DEDF3DA3D372
SHA1:	FF67FCADDA5993CFAA69296AEFCF155893C279EB
SHA-256:	3045F06E40C928526C531FEF56D0EF172C7B45CDAC87D59A81073D4F10A2CE9E
SHA-512:	54AB45588862D5AAF79B609EA8F52430926F354C530BB1166383861F0FE0C3235548351A1DFD270C6A24822B5DEEB543FF85B4DCB54FA35B44E1F051514ED679
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.1.0.7.8.3.1.9.1.0.5.4.3.1.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.1.0.7.8.3.2.2.9.6.4.8.1.4.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.0.8.9.b.b.7.e.-.d.a.f.3.-.4.7.5.b.-.8.e.9.b.-.c.1.7.a.d.5.1.7.6.5.a.b.....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.=.4.3.7.6.4.9.6.8.-.a.2.a.9.-.4.d.7.d.-.9.d.3.1.-.d.9.6.2.1.9.8.3.7.4.4.c.....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.=.0.0.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.2.0.2.0.1.1.0.9._.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.d.f.0.-.0.0.0.1.-.0.0.1.6.-.8.8.a.1.-.f.e.e.e.d.a.c.5.d.6.0.1.....T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.6.0.2.c.d.a.b.d.2.7.f.6.c.7.d.f.b.c.5.a.d.8.6.2.c.4.0.2.7.a.3.0.d.0.0.0.0.0.4.0.8.!.0.0.0.0.f.e.d.b.7.6.0.f.6.7.f.6.0.0.0.b.f.3.1.1.c.7.6.d.f.f.5.5.c.3.5.b.e.e.d.a.8.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_002.exe_566a661da143f3fc1b192bf169fbb3659a52956_6234ae00_00871c35\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12048
Entropy (8bit):	3.772567716869348
Encrypted:	false
SSDEEP:	192:pwQfqJ3HbcjA+njbttz/u7sUS274ItiRs:jqJbcjVjH/u7sUX4ItSs
MD5:	DE39AECB7DE27D5C6CCFEDEB1BFC6A10
SHA1:	BED09940E0337BC7FE6E839750A76EAFCB260CC8
SHA-256:	98D49983ADF4C7542B44BEDA4D3779862CDB4BF97D390EEF314C2673016DF157
SHA-512:	B48EC3BE49299FD5199199AC3392DE7888CA74C0EA5FAC0C5D172D0C1A63C8E99365453A8D762595662C558A134A7A7D97151FA69680BA698264E9AF0C0859B
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.1.0.7.8.3.3.0.5.4.2.9.2.3.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.1.0.7.8.3.3.5.0.4.2.9.2.3.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.b.b.0.7.c.d.3.-.a.2.9.6.-.4.d.8.c.-.b.6.c.f.-.b.5.c.a.8.7.8.8.6.e.1.b.....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.e.f.d.e.8.3.6.-.f.e.f.2.-.4.5.f.7.-.8.2.3.0.-.d.6.e.4.3.a.d.b.e.c.b.f.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.0.0.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.2.0.2.0.1.1.0.9._.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.d.f.0.-.0.0.0.1.-.0.0.1.6.-.8.8.a.1.-.f.e.e.e.d.a.c.5.d.6.0.1.....T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.6.0.2.c.d.a.b.d.2.7.f.6.c.7.d.f.b.c.5.a.d.8.6.2.c.4.0.2.7.a.3.0.d.0.0.0.0.0.4.0.8.!.0.0.0.0.f.e.d.b.7.6.0.f.6.7.f.6.0.0.0.b.f.3.1.1.c.7.6.d.f.f.5.5.c.3.5.b.e.e.d.a.8.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Nov 28 23:05:31 2020, 0x1205a4 type
Category:	dropped
Size (bytes):	62728
Entropy (8bit):	1.8912382117232474
Encrypted:	false
SSDEEP:	192:5llPvcmIwARaNqcYmN5x3qjlGtadY/xIKV/pkHa7ILDz9rGEUi1Tx7:lvcsAkg0N5x6GoW/x7Bq/kSX
MD5:	72AFCDBE07E222E0A9B13E1C9FC83751
SHA1:	0195A8A0CBB567E43903653126F7F16104D955B4
SHA-256:	F37A52664590A33123433479536BF9FA30DC9A5AD6A38B5BD8D188DD682BF356
SHA-512:	7D60C593C601FD6309714F70B467DCB08D91BA90F62F366BB4F8E8B7D232B2019F35AEF56015E7336855DBFD4513EA0321F047FCD6411986D948226EBF2B27B4
Malicious:	false
Preview:	MDMP..... ....._.....U.....B..... .....GenuineIntelW.....T....._.....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\WERA45.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):	8286
Entropy (8bit):	3.703844921832443
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	
SSDEEP:	192:Rrl7r3GLNir66p6YC369gmfjSBCpDK89bN/sfEvm:RrlsNim6p6Y669gmfjSCNkfh
MD5:	5E1680D58C9310366B58FA0BECDE2CDE
SHA1:	E1A2403D1DA40605DC82418454C57961B5534B1E
SHA-256:	A736E83BA14E746424058B6CDB09DAE60E5F207757AE6E35ADDD170736F1B50A
SHA-512:	8CDE417E7F9220421F3A7B42464A240171D0D42647151B6B243C0F509CEBD7B8B78610F14F8B331FCE4751E94462BFD7C86261BC990AA96DC36C227415AC767A
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.>.3.5.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD05.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4628
Entropy (8bit):	4.463401774562659
Encrypted:	false
SSDEEP:	48:cvIwSD8zsVJgtWI9b7WSC8BnM+8fm8M4JsIhFFdI+q8OKaD4Evgqbd:uITfvkKSN8JBrIrB4Evgqbd
MD5:	719846863F13CDFE6A4B6C2AD6340F65
SHA1:	E1A00C1AF960014F33D14771CD7541BAAA7D8E8D
SHA-256:	75E86458817096DC98B0A6844DBFEF3A5BD125BE2F9BC4E26012DFB0F501513C
SHA-512:	0A6CEC446C4F3032C32DEB12C34BBD87C38DAC3BB423D6FD619F7FDC9B431940411BA930523B1830453D50544EE7E19758F07C4562530EE80E057B1C8D20571
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="749296" />.. <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\WERD78B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Nov 28 23:05:20 2020, 0x1205a4 type
Category:	dropped
Size (bytes):	66612
Entropy (8bit):	1.9820330049632604
Encrypted:	false
SSDEEP:	192:K1Oc59bDqecmIwARaNqcYmN5x3T4Fb8C6adY/xIKV/pmyx+mw/KOtuaG/SeOjr:8HyecsAkg0N5xcFbF1W/x7BmyCdjeo
MD5:	E24FB2EEBF67A573571B8420646E8774
SHA1:	2AE347D084DD202B1A480B0AD80C90EEA9C33C37
SHA-256:	D0D2A8D25A43130FC1DE5786080F531584F128E4D3125A4E7AB9BEC0D2EE916B
SHA-512:	9D7EBA878D08508AD2120E670E97463E7CFDDB0986ED0DE82DDA63C71C8E6E27B58BDC65679082C79A248241CB4D3B61673CFDED2E492F87C4E8739872C3751
Malicious:	false
Preview:	MDMP..... ....._.....U.....B..... .....GenuineIntelW.....T....._.....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\WERDD97.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):	8286
Entropy (8bit):	3.7043446739903163
Encrypted:	false
SSDEEP:	192:RrI7r3GLNirZ6Nz6YCM69gmfXS5d6XCprI+89bO/sfaam:RrlsNiI6J6YJ69gmfXS5MCOkfO
MD5:	A97C062B460F1282B1C3003BD4B5DAC7
SHA1:	11ED92911321C80907CAD4BAD55F14D41F4FDAB8
SHA-256:	452040C59F65042A6FFC4031A66170F9E053F2C999B2384D7320B17666DF5460
SHA-512:	C8F443B8AEB190FA5E5C6755CF5D0CA0DC1624512DD37CBFF3FC5F5D2A5E1EB065470CC34F13E6BE5591FFE315BE11F8C8CD9C18E8CF45AAB7AFC58094AFF53
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	
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.>.3.5.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDFCB.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4632
Entropy (8bit):	4.468168107337762
Encrypted:	false
SSDEEP:	48:cvIwSD8zssJgtWI9b7WSC8BU8fm8M4JssZFt+q8cD/4Evgqbd:uITfqkKSNDJtxr/4Evgqbd
MD5:	69934B4EA55B849D6507300552AD293F
SHA1:	8254DD228E1685D7AACA7F54F3C5F2A284F4B2C8
SHA-256:	A84AB5A40CD2F2FE21573ED70246AC8BA492150AC8F0BFE24A6D9086600689CB
SHA-512:	19C3EB1B8AF3FE12B05174DC6068B1E2992AFA85D202764233317C6F8534E72D2B003E8BD6DC235313F0B8C3CD8576AA9DB3132C05CF361BF6C64CCB7287D79
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="749295" />.. <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\sib\{F9266136-0000-46F8-BC66-FDD9185E4296}\SibCa.dll	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	6.867501832742936
Encrypted:	false
SSDEEP:	96:PAWqGuIO1w7JElw764ulqk4uWdCXufAx8Su2yk:oWaIO1S7ulqBhv+yk
MD5:	04F3C7753A4FCABCE7970BFA3B5C76FF
SHA1:	34FC37D42F86DAC1FD1171A806471CDFEAE9817B
SHA-256:	A735E33A420C2AD93279253BC57137947B5D07803FF438499AAAF6FD0692F4CD
SHA-512:	F774FC3F3EBF029DC6F122669060351CC58AE27C5224ABE2A6C8AB1308C4B796657D2F286760EB73A2AE7563EEEF335DAA70ED5E4B2560D34CA9873017658AFE
Malicious:	false
Preview:	..MZ.....0.....8-..@.8.0..p.....!...L.!This. program. cannot .be run i.n DOS mo.de....$...PE..L....d82.....!..0..... ..B..... .....@..*..-.....#.....`....O...+h.....(.Q.....8W.....O.....HA...text.....u.[.....`.rsrc...M;.}.t.....@.0relo...U..).....B.....5...&.....S..4o.....F.....s....(.....*..(....{.%...{.9....[...4.*..("....}....}....A...}....D.}..6..B.(...+**D...* 6..si.....*...0.....,...(.....~.....oRj..*&.....N"(@M.-...on.A..0.....!H.(...o...."r..p(...(.E..r@.po.@.....o.....%.B.....(.@.....o...&..% ....o.x.....u...,..B...o!..B!....!...~...Tu..".[.. ....#E..8...o"..$Q ....c..o....*..*..`.....IT..G.:. `....@;.`.0...`. 5.@.r?..pB1..s#.....A.R.%.r..p.%.DrW...%..*rFq .b*..s....%.o%@.%.oB&....o'...Do(.....o).....".o.>.o+..,oE..,a..+?.,-.@.t.7.a-%o.....Yo/.../.o.].....-...r..../. #"...1..-.....u.>....., ...o2.....#...>....L....X..a"0.$..V..h".r..."3a..r.`.rZ@..p.(4 ....+!rh..c.B..r...po..D.U.*..*.

C:\ProgramData\sib\{F9266136-0000-46F8-BC66-FDD9185E4296}\SibClr.dll	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	52520
Entropy (8bit):	6.011934677477037
Encrypted:	false
SSDEEP:	1536:9GyM4uxlvOe/c1xpfLIa97v3A5KobiPWh:9G1vt/g7fLb97Y5VmY
MD5:	928E680DEA22C19FEBE9FC8E05D96472
SHA1:	0A4A749DDFD220E2B646B878881575FF9352CF73
SHA-256:	8B6B56F670D59FF93A1C7E601468127FC21F02DDE567B5C21A5D53594CDAEF94
SHA-512:	5FBC72C3FA98DC2B5AD2ED556D2C6DC9279D4BE3EB90FFD7FA2ADA39CB976EBA7CB34033E5786D1CB6137C64C869027002BE2F2CAD408ACEFD5C22006A1FF34
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

C:\ProgramData\sib\{F9266136-0000-46F8-BC66-FDD9185E4296}\SibClr.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...d82.....!..0..... ....@..... .....O.....h.....(..... .....8..... ....H.....text..... ....`.rsrc...h.....@..@.reloc..... .....@..B.....H.....S..4o.....F.....s....(....*..(....*..{....*..{....*..{....*..{....*..(.....}.....}.....}.....}....*6..{....(...+**..{.....*6..si... .....*...0.....(.....~.....oj...*&~.....*N(....-.~.....on...*.0.....(....o.....r...p(....(....r...po.....o.....%.~.....(.....o....&.....o .....u....,.~.....o!...on... ...!...~..u....,.~.....o !...on... ..."...[..u....,.~.....o!...on... ...#

C:\ProgramData\sib\{F9266136-0000-46F8-BC66-FDD9185E4296}\sib.dat	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe
File Type:	data
Category:	dropped
Size (bytes):	1864
Entropy (8bit):	4.118434704813
Encrypted:	false
SSDEEP:	48:DAC+SWx9cbv+eufJft0II/PD3Ccb2/SG+Df:DA3locxlX8ryxSG+
MD5:	04D0BDDEDBBC170CF791228E77032526
SHA1:	BF83D0C38B89D40CB72B63C4F1E74334F11B20D7
SHA-256:	B8571739BDAE473B25C929F9033087B3DCCDC84BBA6DC06586CEAD7C39A39123
SHA-512:	A0FFB05A1F8474AAE9FDB470ACF4DF918332C31B85C3CA7D7B8EF8D8599F058EDBFC374B9C49E7570D7A61F1E8A0A0B3B0CBF22ACA1416C35F03F7FB010D40 62
Malicious:	false
Preview:	...&{.F.9.2.6.6.1.3.6.-.2.C.E.2.-.4.6.F.8.-.B.C.6.6.-.F.D.D.9.1.8.5.E.4.2.9.6.}.....p.1.....a.d.m.i.n.....0...0...0.....l.:.\.n.e.w._.k.i.l.l.\.p.1.\.e.x.e.....p.1.(.3.)... e.x.e..E.{. "appVersion": "6.0.8",. "arpNoRemove": true,. "arpNoRepair": true,. "arpNoShow": true,. "lang": "en-US",. "productCode": "{F9266136-0000-46F8-BC66-FDD9185E4296}",. "uiScriptTest": false,. "uid": "{4401C0A1-7F46-4838-BBE8-B6F17E74AA74}",. "upgradeCode": "{9AC75AA0-89B9-4E79-86B4-89 FBE7867A1E}".}...!%.S.y.s.t.e.m.R.o.o.t.%.\.S.y.s.t.e.m.3.2.\.S.H.E.L.L.3.2...d.l.l.....&{.F.1.7.5.3.6.5.4.-.C.5.F.7.-.4.7.C.C.-.B.1.E.D.-.1.E.7.D.D.7.5.C.E.4.8.F.}.....s.e.t.u.p.....l.:.\.n.e.w._.k.i.l.l.\.p.1.\.s.e.t.u.p...e.x.e.....T.e.m.p.\.0.\.s.e.t.u.p...e.x.e.....-.s.....]{."ignoreFailure": false,."uiDisabled" : false,."uiHidden" : false,."uiUnSelected" : false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\002.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Setup.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	135
Entropy (8bit):	5.045303121991894
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUCztJXILKNUhh+9Am12MFuAvOAsDeieVyn:Q3La/xwczflWW+P12MUAvvrs
MD5:	BB527FDBC763485B0662FCCFD53AA00A
SHA1:	86438ECBAF308B24FA264C7B6ECECDABD1338DC0
SHA-256:	6158C0B5B794617AAD8DA6D671FEF9EDE9CAB2AA9A9FAD91D038739DFF5CEDBD
SHA-512:	2003E36806330552D7DD5E633F24A67F2F4226C12EE43A6F79BB709727DD52910CA5EAF336F9C1E5733C66BC3075CA24CACA19D086BE373B76AA08D3FA81810
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.JScript, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\85F91A36E275562F.exe	
Process:	C:\Program Files (x86)\ujvqkl7ofji6\aliens.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	411041792

C:\Users\user\AppData\Local\Temp\85F91A36E275562F.exe	
Entropy (8bit):	0.15732403368611694
Encrypted:	false
SSDEEP:	
MD5:	1B22D5DB9CD16098D4B8B38398029F4E
SHA1:	5E3CD7DE596C320A9F44F37703C787FEA211639C
SHA-256:	718E0B71FAE3F0273BF839E47814143B25D83ADDF2E15A90488E7883FE6077BC
SHA-512:	22F35D101C8ACD939258E2ACC4137AC0CBCB79422E9F16E336194A7DADB18B65FE19DA9A37D7D6E812E39E1C9C799C95069FDCAC36A0C9D3D68793F2DED3150
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....3.!This program cannot be run in DOS mode....$.....-...i.i.i..9.k.`.:.w.`.,...`.+.P.N%.c.N%.H.i.d.`. ./.w.:.k.w.;.h.i.8.h.` .>.h.Richi.....PE..L.....K.....#.....@.....c..... ....@.....@.....@.....<...T.....P..... ....@.....text..... ....rdata..\.... .....@..@.data.....h.....@....rsrc...P.....H.....@..@..... ....

C:\Users\user\AppData\Local\Temp\RarSFX0\002.exe	
Process:	C:\Users\user\Desktop\KeJ7Cl7flZ.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1306112
Entropy (8bit):	6.779030665912039
Encrypted:	false
SSDEEP:	24576:dbM2T9m39cm3+dAu/+jmxsh6QlSfaf0+MHueYujiRDAV0w0I4r:5bTcmm32JrYlSCfziK+0w
MD5:	6503C9C4F19A4B33B701CC5B97B349BC
SHA1:	FEDB760F67F6000BF311C76DFF55C35BEEDA8B81
SHA-256:	B79D5E0C3939BB3DD877DD327AF8D16A9406D8ECA0B888938A0AD39B56311C1A
SHA-512:	641629267461AE617BB639BE4A1C4498FE0AEA101B447A9CF1FC78140A6194992DE3E60A2EB936001226DC088248ED37254D39914F5D0DCED1351C9039823BF6
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Ft.....Q...Q...Q..OQ...Q..FQ...Q..GQ...Q..XQ...Q..CQ...Q...Q1. .QDDWQ...QDDhQ...QDDiQ...Q.GmQ...Q.GSQ...Q...Q...Q.GVQ...QRich...Q.....PE..L.....v.....6.....@.....`.....@..... .....{.....?.....TG.....p%..@.....text....u.....v..... ..`.rdata.....z.....@..@.data...` ....@....rsrc....?.....@...f.....@..@.reloc..TG.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\RarSFX0\BTRSetp.exe	
Process:	C:\Users\user\Desktop\KeJ7Cl7flZ.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	163328
Entropy (8bit):	6.766041496975016
Encrypted:	false
SSDEEP:	3072:F/lD4amo19XRWkv4bOI67IKI1LP6nVqQDSAH6h:rDQo19XRKqI+Ip1LwzWAH6
MD5:	6A6B5428C65FAEA27AC602D0C817476C
SHA1:	849ECCDB3097FAC7368587E4688153D80A5E3A8B
SHA-256:	C2B40AA7A76A98A5DB6C8C5BC02EEA5A25321188A149F6ECEE61EEA189BBC8BD
SHA-512:	04AEDC253EDD23A18D8D563ADFEC5B234A2825AFA92CF3686244875E3E4B5BE17EADB25C6F4C58F40827E6D664F49BAEB2B34AB9F72A2BC83AAB20B485608787
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....h.....`... ....@.. ..... ..... ..@.....g..S.....`..H.....'"^qcJ\p..#... ...$.....@....text...he...`...f...(..... ..`.rsrc.....@..@.reloc.....z.....@..B.....|..... ..`..... .....

C:\Users\user\AppData\Local\Temp\RarSFX0\John_Ship.url	
Process:	C:\Users\user\Desktop\KeJ7Cl7flZ.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<https://iplogger.org/1TT4a7>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	117
Entropy (8bit):	4.778776889587684
Encrypted:	false
SSDEEP:	3:J25YdimVVG/VClAWPUyxAbABGQEZapfdCCAvKoXEL:J254vVG/4xPpuFJQxdCCASoe

C:\Users\user\AppData\Local\Temp\RarSFX0\John_Ship.url	
MD5:	6670D1A3C9071DC7B0748F6818D7E1C3
SHA1:	AC02276BEC28157218DB0159BF83D85677ECF0DD
SHA-256:	6FA22C19F62054C0B6590112081AAF3217965C0216A029DE6390A2ECA7720F9B
SHA-512:	9433541797F6CB4AB93EA1B22A355030113C6131473C536DBFA52876D8928EDD0C160B05856849C9012A1EB8C67D2DFD8CE2E5DEDB2A1D6FF915103FC3E0947
Malicious:	false
Preview:	[{000214A0-0000-0000-C000-000000000046}]..Prop3=19,11..[InternetShortcut]..IDList=..URL=https://iplogger.org/1TT4a7..

C:\Users\user\AppData\Local\Temp\RarSFX0\SSSS.exe	
Process:	C:\Users\user\Desktop\KeJ7Cl7flZ.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	308224
Entropy (8bit):	4.340693708730459
Encrypted:	false
SSDEEP:	3072:L3Vi8CzqGLI9F5NXgDJUnPms7U158fRWG0zn2tMbfcPRGCMjjjjjjjjo:OOGLI9lXUJ+Pms7d8G42tMbfcPRGCM
MD5:	7285B1F8E710E7D686F70306A76AD055
SHA1:	2D038C234C65B19B118C9820A917BA70E3623C18
SHA-256:	3DD96A30CF8E7A4E3E4E5FD64F4F71B78CE51F05C0B2DBB776D2CE4179ED7EA9
SHA-512:	A2B4C4F8AF7541409ECA18FCEEF718CEFAA6B8FA08222CA68BE30931AD7582F35D576CEF8C66EC3293EBE014FC8F1443F45A723437D84F70AAD3AA082D7A22BF
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L....el].....^+.....\.....@.....,...&<.....<...<.... +.....,..... .....text..... ..`.data.....)....4.....@....vuwuzed.....+.....0.....@....sudoze.....+.....2.....@....rsrc..... +.....4.....@..@.reloc..p... ..,.....@..B..... .....

C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe	
Process:	C:\Users\user\Desktop\KeJ7Cl7flZ.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4240136
Entropy (8bit):	7.970247718055294
Encrypted:	false
SSDEEP:	98304:YjIeXG3LvUm3JyHGLjR+OCyn8LmqsQf4xi3OimS1gHNQd4yN:YjAAF2jR+68LmJ24xITCtQj
MD5:	62EAEA103DD9BEB69E884F2EDE1ACD63
SHA1:	324DB9E359DA3489217C5CB2F46B59AD383C8523
SHA-256:	E1A1205CC671D2008D09ED556DB705D3F3976B8098C4E2304C6E6C84041C22B8
SHA-512:	B501AF99056DA3D34EE27F63548C89F9C9157182C55838FAE26F510C88E2FA2105E083766F270F41B661E6306EB78D3B2D26BE3B7C2A9E0EF55B7FDF212BD94D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A{.k...8...8...8.b<8...8.b,8...8...8...8...8...8..%8...8.."8...8Rich...8 .....PE..L.....GO.....t...z...B...8.....@..... .....@.....@.....@.....`..... .....text....r.....t..... ..`.rdata..n+.....x.....@..@.data....+.....@....ndata...P.....rsrc.....@.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\RarSFX0\askinstall21.exe	
Process:	C:\Users\user\Desktop\KeJ7Cl7flZ.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	536576
Entropy (8bit):	6.856117131435329
Encrypted:	false
SSDEEP:	12288:RXvt5Xy3dte25VTD21EOj5Ia4c9co+3aag9dCj6pr1FWZGKSu9mJeoBL:R12T61E4IfXi95ndu9e
MD5:	3B7666DDCD8668A6E0F228BC15C2D528
SHA1:	1EC26D6AFC64C30291A12638F9FA1CACBC530834
SHA-256:	FF7C1BE25F9D0B351C2F1F11B9700D6C467519F6E374DF66A78DB855EAC39DD9
SHA-512:	21730DF8C6450F304926C0F81B2C1352563127FA353C4A05B32EA03C3950D65DAAA83B684C27F31334BF7C00B99CA49CAE508FCC2EF93AD1BF70B57310898995
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\AppData\Local\Temp\RarSFX0\askinstall21.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._..V.h...h...h..~....h..~....h..~....h..I....h..I...Yh..I...9h..~....h...h...h.... ...h....4..h...h\..h.....h..Rich.h.....PE..L...`..\_.....>.....@.....@.....@.....x....`..`.....`...<.....p..... .....@.....8.....text...t..... ....vnnsfgf.=.....>..... ..`.vnnsfgfz.... ..... ..`.vnnsfgf.....0..... ..`.vnnsfgf.....@.....\*.... ..... ..`.vnnsfgf>....P.....,..... ..`.vnnsfgf.....p.....>..... ..`.rdata.....B.....@..@.data...P)...0.....@....rsrc...`....`.....@..@.reloc... <...`...>.....@..B.....

C:\Users\user\AppData\Local\Temp\RarSFX0\config.ini	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\002.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	3
Entropy (8bit):	0.9182958340544896
Encrypted:	false
SSDEEP:	3:f:f
MD5:	93DD4DE5CDDBA2C733C65F233097F05A
SHA1:	6FC978AF728D43C59FAA400D5F6E0471AC850D4C
SHA-256:	A1DD6837F284625BDB1CB68F1DBC85C5DC4D8B05BAE24C94ED5F55C477326EA2
SHA-512:	FA3AD36CF41C6AF0E9EC7CCFDB69276D67F5C5F99D09064DC565FCDE761E7D9F7FD2AE45DFD8487C89AFF5BBCC11B58EBF44D5C22F114249B3CA4A6E088B 2B2
Malicious:	false
Preview:	002

C:\Users\user\AppData\Local\Temp\RarSFX0\d	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	26824704
Entropy (8bit):	0.9757760335200523
Encrypted:	false
SSDEEP:	24576:5ELvckxfUgj2h9yr9YN/3kOunAPQoqooiO3PX2BU:eUgj2h9uYNPkOuQ
MD5:	E13008D82626E15656E9AB26F4901C17
SHA1:	A25AE485F4A14A6A04C9CCE1737FF9BF9E93DADE
SHA-256:	1446D4AA481B61982A52DFE5326B52B2CD8A4D8A7A33BC258D79FC024C908379
SHA-512:	B68A2FE17DDCC8F03B83D7F87785CABD10A8710E6E1A48183612D9228BDBECA79471556BB620BA89E06EEAB1B435DF899186DE36F4DF1131CFC596755E850D 8
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\RarSFX0\d.INTEG.RAW	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1605
Entropy (8bit):	5.206056345547401
Encrypted:	false
SSDEEP:	12:KuiC4ts26Fp23tnungHQCbcMU/NVlyax4dKJ1qUtLnFtAO71OZ1OOynuQL1h9uqn:K24CX7utbFU/fljPtt7cPy51huh3s
MD5:	D2A0EA84FB0A10722D869674BF875F53
SHA1:	CC2B9DDECF88BE8062DAC7B93EF742E251D9F5E6
SHA-256:	7AC1ACC412CFE6C754B0431A8A62F0EDA213DA1EB32584ED0D8FD2776A49AD8F
SHA-512:	B6BA7BF26E388E4DE069333E2094BB409F96D273CF049ECC421796589095DCAAB26703695CB26E3E9200C563DD99AE5D156D99B4DFE243AA6EE3F96942F9AEE 0
Malicious:	false
Preview:	***** Repair of database 'd' started [ESENT version 06.02.9200.0000, (ESENT[6.2.9200.0] RETAIL RTM MBCS)]....search for 'ERROR:' to find errors..search for 'WAR NING:' to find warnings..checking database header..ERROR: database was not shutdown cleanly (Dirty Shutdown)..database file "d" is 26738688 bytes..database file "d" is 26738688 bytes on disk...Creating 16 threads..checking SystemRoot..SystemRoot (OE)..ERROR: page 2: dbtime is larger than database dbtime (0x3844, 0x3172)..SystemRoot (AE)..ERROR: page 3: dbtime is larger than database dbtime (0x3846, 0x3172)..checking system tables..MSysObjects ..MSysObjectsShadow ..M SysObjects:.5056:.ERROR: page 13: dbtime is larger than database dbtime (0x37e0, 0x3172)..MSysObjects:.5056:.ERROR: page 19: dbtime is larger than database dbti me (0x37f8, 0x3172)..MSysObjects:.5056:.ERROR: page 20: dbtime is larger than database dbtime (0x3899, 0x3172)..MSysObjects Name..MSysObjects RootObje cts..MSysObjectsShadow:.5056:.ERROR: page 27: dbtime is larg

C:\Users\user\AppData\Local\Temp\RarSFX0\d.jfm	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\RarSFX0\d.jfm	
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.07621424775336932
Encrypted:	false
SSDEEP:	3:iTmARoM/ClAJOwYGll/zG6B/ill:iT2AJOHG//BE
MD5:	20F07AEBA37DAA75B58799DCEB795F56
SHA1:	041A1C528F83EF16889B529CB94BE1A19EB99254
SHA-256:	B1B88CC6BB90D79D746CA4CFCCAD43F07F775340575115CAD1BC49B48D633BDE
SHA-512:	CAEE3277934685EA0EF993876C082221548F667843E7D73030446F2102B085066678482A1578FF5B634695297D202FFA907FFE28521A915E945CE3E0BB51D7DE
Malicious:	false
Preview:	?.....x+.....x+.....x.....#.....x+..... ....

C:\Users\user\AppData\Local\Temp\RarSFX0\file1.exe	
Process:	C:\Users\user\Desktop\KeJ7Cl7flZ.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	197104
Entropy (8bit):	5.334591854768522
Encrypted:	false
SSDEEP:	3072:kWsKHzuQmpEARYFlUJMym6tiWIZqU18x5w48qTdnuC61:khKTuDMFatTddE
MD5:	F542EE32E7168671E2952B89BE66BCA3
SHA1:	C3E785978EA1747182D3C153CBB39089E522A4A1
SHA-256:	8EE3A19D5E1A6C198E6AD759C697910D681365A638ACE0BC9E9C622AFE16BC73
SHA-512:	2C8C5FD5B0267F750809D2BAB24EBE070D11649CF2C827661C78C6627C8D7FC3B1375FDA43079DD7DAB21A02F5D75B9423F044203F58AEACE78C4F89D23C64B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W...W...W...8.9.^...8...^...8.8.`...^...P...W.....8.=.U...8...V...8...V...RichW.....PE..L....I._.....R..... .....p....@..... .....<.....@.....P....P.....#..... ...@.....p.....text....P.....R..... ..`.rdata..^!...p..."...V.....@..@.data.. .....x.....@....rsrc.....P.....@..@.reloc..B..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\RarSFX0\hjjgaa.exe	
Process:	C:\Users\user\Desktop\KeJ7Cl7flZ.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1001984
Entropy (8bit):	7.363053750938072
Encrypted:	false
SSDEEP:	24576:GSmPzwRTwg3dqOdzz8E8yg2Nr+r+qdTNkdBAnlXG6+Z1mbXHIH:uLg3dqOh8EPg2p+r1kUlXF+Z1IYH
MD5:	5AF45B49951E4E3B1C6D1A0B9CBED2DB
SHA1:	CAE3F32B485F8406D8C4FB9AEECEB923B94B9452
SHA-256:	86407608F44BB780D40B92E45B200EDB584395CA6536E172149C75FA8C60FC5E
SHA-512:	F4DFCD7A5DA8458FC5727DF712FEE1E14BE0B9C9FC0B14DD31C8BC10AB85E469D975C2D4982D031901ABB1BABA10DB3976B58E4D66BE1094DC79FFF04D4A074B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Ee.$...$...$...L...$...L...$...L...$..(C...$..(C...$..(C...$...L...$...$...$...I...$...I.$...$...$...I...$..Rich.$.....PE..L....._.....2...&.....P....@.....@.....d.... .....@...N..`P..p..... .....tQ.....P..@.....P.....text...P1.....2..... ..`.rdata.....P.....6.....@..@.data....6.....&.....@....rsrc..... .....@..@.reloc...N...@...P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe	
Process:	C:\Users\user\Desktop\KeJ7Cl7flZ.exe
File Type:	MS-DOS executable, MZ for MS-DOS
Category:	dropped
Size (bytes):	574976
Entropy (8bit):	7.836549545044653
Encrypted:	false

C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe	
SSDEEP:	12288:8dyQUaL0a2eSteSPFRLbsY/hhgKXmEuIzRP/IYLkbQVBMvtAdhKuD:syQTLcTUGAhILzpIkkCMvShX
MD5:	676757904C8383FD9ACBEED15AA8DCC4
SHA1:	63F219EC9EF458A258B1845F42D46D2B12F30E8A
SHA-256:	B44ACC4498924F5FA6A479E263626E3A36FEE380C6D7463269BC5054DC64C4A9
SHA-512:	A4D4C945D334153FB91F2736A1EF20F6C4B5C710EC7E2064CDEF503D926BB5DA16F6ED32C56D2FC94EBB0F75BE5E25E0C4CF13E8F9A8F2FD2F110B547AEC0845
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ@.....!..L.!Win32 .EXE...$@...PE..L....b._.....r.....@.....`.....p.....\.....P.....@.....MPRESS1.....MPRESS2p.....rsrc...\.....@.....v2.19..... ..5...5.|..y...#Vr..n!r..D&..7....z!ST.z..8...s.K..q9.....{M..1.l....b..C.v....Q.3..b.....E.7._../.....8.uq...;....Y..wclE.....g....I...s.S....4 .I.....<j7X..R....y....h..k..m{.2-[.SB0.ZX//..Au..xi....:e`x.9.Z...].q._Ui_y..^.{.I%U-.>....{.{S..Ic=1|...G.T....oY/.....w..e..d..W%.A../l.G{.Z...."....-...s.LI.YA[.I7...2!...z.8..m..j..2".x..@..T..... .....V.^./.....p.Ex.~.&.T.o.a.yT.....r=.|..8.l...3...x.Do.Rt.....a..f....y.4..

C:\Users\user\AppData\Local\Temp\RarSFX0\tmp.edb	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x67bf4a01, page size 32768, JustCreated, Windows version 0.0
Category:	dropped
Size (bytes):	163840
Entropy (8bit):	0.3131370344992014
Encrypted:	false
SSDEEP:	6:Jb80jDb80jztv0sRt+lsWtktlclPktktktktktktktktktktktktktktktk8:Z80jH80jz1X7aNfvaXXXX
MD5:	90FCF86F736C8FE6ECAA12619E61CB2C
SHA1:	7CE6019618F2EB4CB1A90062D2EE064290D242B8
SHA-256:	EF996B450CD717FC6C98F57E141FE46EC09D6399E6741E27F112DA679BF21380
SHA-512:	8404C1BE071D57381E87E278BA956278182D46CAD0A4354EAEF48F89DF43E5FE7E37ADE99839A19BDE5878C3C997DA0CDA262A2A7D95BF25644EDCDADDB997C
Malicious:	false
Preview:	g.J.... .....@.....vI.....x..... ....0I.....x..... .....

C:\Users\user\AppData\Local\Temp\RarSFX0\ubisoftpro.exe	
Process:	C:\Users\user\Desktop\KeJ7Cl7flZ.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1811968
Entropy (8bit):	6.726904896911865
Encrypted:	false
SSDEEP:	49152:O6NxkuveGb4EurlP8cQFtYiSoTZipZnXwm:WuveGMZ8cQF6n
MD5:	D8AD7E3F18ED1A10211643FC215C1C26
SHA1:	7878E78F38FE8D181121B967271B69688EB56FC0
SHA-256:	B5CACBDB1C527613FFAA6CBCDDAFF819CC1AFC5EFEC0F914B9CEA1F65C1E3FD7
SHA-512:	203751424C86427AFA1E5F59509412186133F57949FFDFA92FCCA14D1BAFAF6710127F409140B2DEDB25F89C9BB1EC1BA47F25A6B6B4D3CB4E753DE842F4DF9
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&i..H:..H:..H:...:..H:...:..H:...:..H:...:..H:...:..H:..I:a.H:...:..H:...:..H:..:[.H:...:..H:...:..H:...:..H:Rich..H:.....PE..L....._.....>.....P....@.....0.....@.....`5..h....@..p.....0.....@...@.....P.....3..@.....text...e<.....>..... ..`.rdata.....P.....B.....@..@.data.....`...z...N.....@....rsrc.....@.....@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsq2FFD.tmp\Sibuia.dll	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	540456
Entropy (8bit):	6.4900404695826275
Encrypted:	false
SSDEEP:	12288:GUBa9WxfxYRW3vwDaduy2NBCzrCJDVxsR7LafByUb2iqyTOHD:da9WxfiRCv2anZnXtLa32idOHD
MD5:	EB948284236E2D61EAE0741280265983
SHA1:	D5180DB7F54DE24C27489B221095871A52DC9156
SHA-256:	DBE5A7DAF5BCFF97F7C48F9B5476DB3072CC85FBFFD660ADAFF2E0455132D026

C:\Users\user\AppData\Local\Temp\nsq2FFD.tmp\Sibuia.dll

<table>
<tr><td>SHA-512:</td><td>6D8087022EE62ACD823CFA871B8B3E3251E44F316769DC04E2AD169E9DF6A836DBA95C3B268716F2397D6C6A3624A9E50DBE0BC847F3C4F3EF8E09BFF30F2D
5</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>MZ......................@..................................(...........!..L.!This program cannot be run in DOS mode....$.......A.....}...}...}^..|...}...|...}^..|...}^..|...}^..|...}^..|$..}...}x..}...|...}...|...}...|z
..}...|...}...|...}..?}...}..W}...}...|...}Rich...}.......................PE..L....mU_...........!.....2..................P.......................................8....@.........................@...\..............."........... ..(....0..L
H..X(..p....................).......(..@............P..............................text....1.......2................. ..`.rdata...]...P...^...6.............@..@.data....I..........................@....rsrc...."........$.........
.........@..@.reloc..LH...0...J.................@..B...
....</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\sib309A.tmp\0\setup.exe

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3956884
Entropy (8bit):	7.9692463026726985
Encrypted:	false
SSDEEP:	98304:MoxQvFZ6eRJK3WbxBaOiKH2v6Ks4pmf6pK6Iir6l3C36+a:4yn2xBayWv6Jgmf6ROxC4
MD5:	D64E3CC11AFC6331715BDFEC5F26C2A0
SHA1:	BA606F3C9115C584A902C909AC82F411463B551A
SHA-256:	4C02D9BCAE00635DF67EA4D3D64C67F258F0256C9F1553997815F8702BC34C63
SHA-512:	DA002E155D6BAF03648576A4574EA4635BD35ADE04EA0175F3F406895085CD1DA9A19EB0E19E0445D40C7D6E2A42D613F0D65684775022AD426DB840034448CE
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......b`..&...&...&.....h.+.....j.......k.>.....^.$...._..0...._..5...._......./y..,.../y ..#...&...,...._......._..'...._f.'...._..'...Rich&..................PE..L....~.^.................................... ....@.........................0............@............................4...4...<.... ..p.......................d".... ..T...........................D..@............ ..`....... ....................text...*.......................... ..`.rdata...... ....@..@.data... 7.........................@....didat.............................@....rs rc........ ....@..@.reloc..d".......$.................@..B... ....

C:\Users\user\AppData\Local\Temp\sib309A.tmp\SibCa.dll

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	6.867501832742936
Encrypted:	false
SSDEEP:	96:PAWqGuIO1w7JElw764ulqk4uWdCXufAx8Su2yk:oWalO1S7ulqBhv+yk
MD5:	04F3C7753A4FCABCE7970BFA3B5C76FF
SHA1:	34FC37D42F86DAC1FD1171A806471CDFEAE9817B
SHA-256:	A735E33A420C2AD93279253BC57137947B5D07803FF438499AAAF6FD0692F4CD
SHA-512:	F774FC3F3EBF029DC6F122669060351CC58AE27C5224ABE2A6C8AB1308C4B796657D2F286760EB73A2AE7563EEEF335DAA70ED5E4B2560D34CA9873017658AF E
Malicious:	false
Preview:	..MZ.........0......8-..@.8.0..p.........!...L.!This. program. cannot .be run i.n DOS mo.de....$...PE..L....d82........!..0............ ..B.................. ....@..*..-......#......`....O...+h......... (.Q..........8W.....O......HA...text..........u.[.......`.rsrc...M;.}.t.......@.0relo...U..)......B.......5...&......S..4o.......F.......s....(.....*..(....{.%...{.9....[...4.*..(".....}...."}A...}....D.}..6..B.(...+** D...* 6..si.......*...0.....,....(.....~......oRj..*&.....N"(@M.-...on.A..0......!H.(...o...."r..p(...(.E..r@.po.@.....o..........%.B.....(.@........o...&..% ....o.x......u...,..B...o!..B!....!...~...Tu..".[.. ....#E..8...o"..$Q ....c..o....*..*..`......IT..G.:. `....@;.`.0...`. 5.@.r?..pB1..s#.....A.R.%.r..p.%.DrW...%..*rFq .b*..s....%.o%@.%.oB&....o'...Do(..........o)......"o.>.o+..,oE..,a..+?.,- .@.t.7.a-%o......Yo/.../.o.].....-...r..../. #"...1..-......u.>....., ...o2......#...>....L....X..a"0.$..V..h".r..."3a..r..`.rZ@..p.(4 ....+!rh..c.B..r...po..D.U.*..*.

C:\Users\user\AppData\Local\Temp\sib309A.tmp\SibClr.dll

Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	52520
Entropy (8bit):	6.011934677477037
Encrypted:	false
SSDEEP:	1536:9GyM4uxlvOe/c1xpfLIa97v3A5KobiPWh:9G1vt/g7fLb97Y5VmY
MD5:	928E680DEA22C19FEBE9FC8E05D96472
SHA1:	0A4A749DDFD220E2B646B878881575FF9352CF73
SHA-256:	8B6B56F670D59FF93A1C7E601468127FC21F02DDE567B5C21A5D53594CDAEF94
SHA-512:	5FBC72C3FA98DC2B5AD2ED556D2C6DC9279D4BE3EB90FFD7FA2ADA39CB976EBA7CB34033E5786D1CB6137C64C869027002BE2F2CAD408ACEFD5C22006A1F F34
Malicious:	false

C:\Users\user\AppData\Local\Temp\sib309A.tmp\SibClr.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...d82.....!..0..... ....@.....O.....h.....(.....8..... ....H.....text..... ....`.rsrc...h.....@..@.reloc..... .....@..B.....H.....S..4o.....F.....s....(....*..(....*..{....*..{....*..{....*..{....*..(.....}.....}.....}.....}.....}....*6..{....(...+**..{.....*6..si... .....*...0.....(.....~.....oj...*&~.....*N(....-.~.....on...*.0.....(....o.....r...p(....(....r...po.....o.....%.~.....(.....o....&.....o .....u.....,~.....o!...on... ...!...~..u.....,~.....o !...on... ..."...[..u.....,.~.....o!...on... ...#

C:\Users\user\Documents\VlcpVideoV1.0.1\jg2_2qua.exe	
Process:	C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe
File Type:	MS-DOS executable, MZ for MS-DOS
Category:	dropped
Size (bytes):	574976
Entropy (8bit):	7.836549545044653
Encrypted:	false
SSDEEP:	12288:8dyQUaL0a2eSteSPFRLbsY/hhgKXmEulzRP/IYLkbQVBMvtAdhKuD:syQTLcTUGAhILzpIkkCMvShX
MD5:	676757904C8383FD9ACBEED15AA8DCC4
SHA1:	63F219EC9EF458A258B1845F42D46D2B12F30E8A
SHA-256:	B44ACC4498924F5FA6A479E263626E3A36FEE380C6D7463269BC5054DC64C4A9
SHA-512:	A4D4C945D334153FB91F2736A1EF20F6C4B5C710EC7E2064CDEF503D926BB5DA16F6ED32C56D2FC94EBB0F75BE5E25E0C4CF13E8F9A8F2FD2F110B547AEC0845
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ@.....!..L.!Win32 .EXE...$@...PE..L....b._.....r.....@.....`.....p.....\..... .....P.....@.....MPRESS1.....MPRESS2p.....rsrc...\.....@..... .....v2.19..... ..5...5.|..y...#Vr..n!r..D&..7....z!ST.z..8...s.K..q9.....{M..1.l....b..C.v....Q.3..b.....E.7._../.....8.uq...;....Y..wclE.....g....l...s.S....4 .l.....<j7X..R....y ....h..k..m{.2-[.SB0.ZX//..Au..xi....:e`x.9.Z...].q._Ui_y..^.{.I%U-.>....{.{S..Ic=1|...G.T....oY/.....w..e..d..W%.A../l.G{.Z...."....-...s.Ll.YA[.l7...2!...z.8..m..j..2".x..@..T..... .....V.^ ./.....p.Ex.~.&.T.o.a.yT.....r=.|..8.l...3...x.Do.Rt.....a..f....y.4..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.99387668493442
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	KeJ7Cl7flZ.exe
File size:	7922731
MD5:	4e759849412063c6590936671ce4aa0e
SHA1:	40d132516cc4b9aa00dca2b2f068c439cf8f59c3
SHA256:	7a79f0c95e891b939e275fa19e641b676f2eb70471945fb3b15d6a649cafe071
SHA512:	636f2e0049eab66d31a07446dbd9a747931c2ee8954b9878a7133c783e530eeba7b45060ad3bcf2f7e70c96fac4b680650c6c501aabb48cdfe98457535297e91
SSDEEP:	196608:KBYjwbZ5mValPcW4lib2cnmzq3oi7eGhJe+Qc7z11mX6ZnGw:jM5GMxb2cmcoi7Pa8z11mXg
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.k...k..k..c.a..k..c.c.[k..c.b..k..l.W..k...5./.k...5./.k...5./.k.....k.....k...k..!k..@5./.k..@5./.k..E5o..k..@5./.k.

File Icon

Icon Hash:	d49494d6c88ecec2

Static PE Info

General

Entrypoint:	0x413c60

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	GUARD_CF, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5EF47EA5 [Thu Jun 25 10:38:29 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	ae9f6a32bb8b03dce37903edbc855ba1

Entrypoint Preview

Instruction
call 00007FF0987CDBDDh
jmp 00007FF0987CD51Dh
cmp ecx, dword ptr [00431558h]
jne 00007FF0987CD695h
ret
jmp 00007FF0987CDD5Eh
jmp 00007FF0987D20B3h
push ebp
mov ebp, esp
and dword ptr [00465380h], 00000000h
sub esp, 28h
push ebx
xor ebx, ebx
inc ebx
or dword ptr [0043155Ch], ebx
push 0000000Ah
call 00007FF0987E0223h
test eax, eax
je 00007FF0987CD803h
and dword ptr [ebp-10h], 00000000h
xor eax, eax
or dword ptr [0043155Ch], 02h
xor ecx, ecx
push esi
push edi
mov dword ptr [00465380h], ebx
lea edi, dword ptr [ebp-28h]
push ebx
cpuid
mov esi, ebx
pop ebx
mov dword ptr [edi], eax
mov dword ptr [edi+04h], esi
mov dword ptr [edi+08h], ecx
mov dword ptr [edi+0Ch], edx
mov eax, dword ptr [ebp-28h]
mov ecx, dword ptr [ebp-1Ch]
mov dword ptr [ebp-08h], eax
xor ecx, 49656E69h
mov eax, dword ptr [ebp-20h]
xor eax, 6C65746Eh
or ecx, eax
mov eax, dword ptr [ebp-24h]
push 00000001h

Instruction
xor eax, 756E6547h
or ecx, eax
pop eax
push 00000000h
pop ecx
push ebx
cpuid
mov esi, ebx
pop ebx
mov dword ptr [edi], eax
mov dword ptr [edi+04h], esi
mov dword ptr [edi+08h], ecx
mov dword ptr [edi+0Ch], edx
jne 00007FF0987CD6D5h
mov eax, dword ptr [ebp-28h]
and eax, 0FFF3FF0h
cmp eax, 000106C0h
je 00007FF0987CD6B5h
cmp eax, 00020660h
je 00007FF0987CD6AEh
cmp eax, 00020670h

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [EXP] VS2015 UPD3.1 build 24215 • [LNK] VS2015 UPD3.1 build 24215 • [IMP] VS2008 SP1 build 30729 • [C++] VS2015 UPD3.1 build 24215 • [RES] VS2015 UPD3 build 24213

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2ffa0	0x34	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2ffd4	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x67000	0xdfd0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x75000	0x27ec	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x2e810	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x29238	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x27000	0x220	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x2f694	0x100	.rdata
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	0x25f0a	0x26000	False	0.577264083059	data	6.69284076721	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x27000	0x9c14	0x9e00	False	0.453075553797	data	5.20986268254	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x31000	0x34d90	0xe00	False	0.377790178571	data	3.79528519664	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.didat	0x66000	0x15c	0x200	False	0.408203125	data	2.99773455687	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x67000	0xdfd0	0xe000	False	0.637050083705	data	6.63698184983	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x75000	0x27ec	0x2800	False	0.8044921875	data	6.7259837024	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
PNG	0x67650	0xb45	PNG image data, 93 x 302, 8-bit/color RGB, non-interlaced	English	United States
PNG	0x68198	0x15a9	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced	English	United States
RT_ICON	0x69748	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x69cb0	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x6a558	0xea8	data	English	United States
RT_ICON	0x6b400	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x6b868	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x6c910	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x6eeb8	0x3d71	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_DIALOG	0x73588	0x286	data	English	United States
RT_DIALOG	0x73358	0x13a	data	English	United States
RT_DIALOG	0x73498	0xec	data	English	United States
RT_DIALOG	0x73228	0x12e	data	English	United States
RT_DIALOG	0x72ef0	0x338	data	English	United States
RT_DIALOG	0x72c98	0x252	data	English	United States
RT_STRING	0x73f68	0x1e2	data	English	United States
RT_STRING	0x74150	0x1cc	data	English	United States
RT_STRING	0x74320	0x1b8	data	English	United States
RT_STRING	0x744d8	0x146	Hitachi SH big-endian COFF object file, not stripped, 17152 sections, symbol offset=0x73006500	English	United States
RT_STRING	0x74620	0x446	data	English	United States
RT_STRING	0x74a68	0x166	data	English	United States
RT_STRING	0x74bd0	0x152	data	English	United States
RT_STRING	0x74d28	0x10a	data	English	United States
RT_STRING	0x74e38	0xbc	data	English	United States
RT_STRING	0x74ef8	0xd6	data	English	United States
RT_GROUP_ICON	0x72c30	0x68	data	English	United States
RT_MANIFEST	0x73810	0x753	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

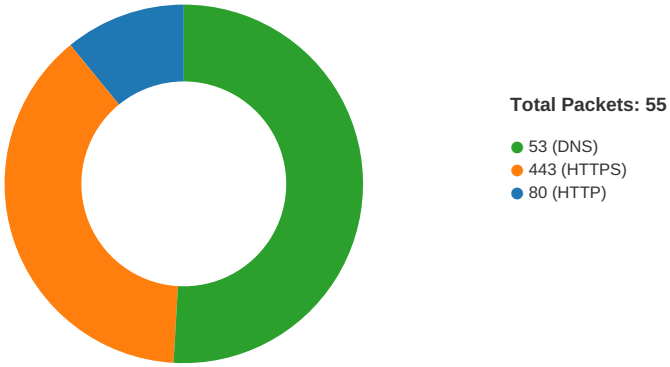
DLL	Import
KERNEL32.dll	GetLastError, SetLastError, FormatMessageW, GetFileType, GetStdHandle, WriteFile, ReadFile, FlushFileBuffers, SetEndOfFile, SetFilePointer, SetFileTime, CloseHandle, CreateFileW, CreateDirectoryW, SetFileAttributesW, GetFileAttributesW, DeleteFileW, MoveFileW, FindClose, FindFirstFileW, FindNextFileW, GetVersionExW, GetCurrentDirectoryW, GetFullPathNameW, FoldStringW, GetModuleFileNameW, GetModuleHandleW, FindResourceW, FreeLibrary, GetProcAddress, GetCurrentProcessId, ExitProcess, SetThreadExecutionState, Sleep, LoadLibraryW, GetSystemDirectoryW, CompareStringW, AllocConsole, FreeConsole, AttachConsole, WriteConsoleW, TzSpecificLocalTimeToSystemTime, SystemTimeToFileTime, FileTimeToLocalFileTime, LocalFileTimeToFileTime, FileTimeToSystemTime, GetCPInfo, IsDBCSLeadByte, MultiByteToWideChar, WideCharToMultiByte, GlobalAlloc, LockResource, GlobalLock, GlobalUnlock, GlobalFree, LoadResource, SizeofResource, SetCurrentDirectoryW, GetExitCodeProcess, WaitForSingleObject, GetLocalTime, GetTickCount, MapViewOfFile, UnmapViewOfFile, CreateFileMappingW, OpenFileMappingW, GetCommandLineW, SetEnvironmentVariableW, ExpandEnvironmentStringsW, GetTempPathW, MoveFileExW, GetLocaleInfoW, GetTimeFormatW, GetDateFormatW, GetNumberFormatW, SetFilePointerEx, GetConsoleMode, GetConsoleCP, HeapSize, SetStdHandle, GetProcessHeap, RaiseException, GetSystemInfo, VirtualProtect, VirtualQuery, LoadLibraryExA, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, GetCurrentProcess, TerminateProcess, RtlUnwind, EncodePointer, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, QueryPerformanceFrequency, GetModuleHandleExW, GetModuleFileNameA, GetACP, HeapFree, HeapAlloc, HeapReAlloc, GetStringTypeW, LCMapStringW, FindFirstFileExA, FindNextFileA, IsValidCodePage, GetOEMCP, GetCommandLineA, GetEnvironmentStringsW, FreeEnvironmentStringsW, DecodePointer
gdiplus.dll	GdiplusShutdown, GdiplusStartup, GdipCreateHBITMAPFromBitmap, GdipCreateBitmapFromStreamICM, GdipCreateBitmapFromStream, GdipDisposeImage, GdipCloneImage, GdipFree, GdipAlloc

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 15:07:10.123815060 CET	49732	80	192.168.2.5	101.36.107.74
Nov 28, 2020 15:07:10.383060932 CET	80	49732	101.36.107.74	192.168.2.5
Nov 28, 2020 15:07:10.383348942 CET	49732	80	192.168.2.5	101.36.107.74
Nov 28, 2020 15:07:10.385420084 CET	49732	80	192.168.2.5	101.36.107.74
Nov 28, 2020 15:07:10.643752098 CET	80	49732	101.36.107.74	192.168.2.5
Nov 28, 2020 15:07:10.647347927 CET	80	49732	101.36.107.74	192.168.2.5
Nov 28, 2020 15:07:10.690886974 CET	49732	80	192.168.2.5	101.36.107.74
Nov 28, 2020 15:07:10.825555086 CET	49733	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:10.847800016 CET	443	49733	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:10.847906113 CET	49733	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:10.852497101 CET	49733	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:10.874772072 CET	443	49733	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:10.876108885 CET	443	49733	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:10.876132965 CET	443	49733	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:10.876152992 CET	443	49733	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:10.876172066 CET	443	49733	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:10.876313925 CET	49733	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:10.989924908 CET	49733	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:11.013079882 CET	443	49733	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:11.050437927 CET	49733	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:11.081525087 CET	443	49733	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:11.081581116 CET	443	49733	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:11.081764936 CET	49733	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:11.213141918 CET	49733	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:11.235768080 CET	443	49733	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:11.237801075 CET	49733	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:15.647485018 CET	80	49732	101.36.107.74	192.168.2.5
Nov 28, 2020 15:07:15.649553061 CET	49732	80	192.168.2.5	101.36.107.74
Nov 28, 2020 15:07:15.657855988 CET	49732	80	192.168.2.5	101.36.107.74
Nov 28, 2020 15:07:15.916197062 CET	80	49732	101.36.107.74	192.168.2.5
Nov 28, 2020 15:07:27.017199039 CET	49737	443	192.168.2.5	88.99.66.31

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 15:07:27.039550066 CET	443	49737	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:27.039808035 CET	49737	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:27.042964935 CET	49737	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:27.065248013 CET	443	49737	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:27.067945957 CET	443	49737	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:27.067984104 CET	443	49737	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:27.068008900 CET	443	49737	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:27.068033934 CET	443	49737	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:27.068073034 CET	49737	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:27.068104982 CET	49737	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:27.082701921 CET	49737	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:27.106343985 CET	443	49737	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:27.106636047 CET	49737	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:27.109718084 CET	49737	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:27.141027927 CET	443	49737	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:27.141211033 CET	49737	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:35.965049028 CET	49737	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:35.992804050 CET	443	49737	88.99.66.31	192.168.2.5
Nov 28, 2020 15:07:35.992925882 CET	49737	443	192.168.2.5	88.99.66.31
Nov 28, 2020 15:07:36.034851074 CET	49737	443	192.168.2.5	88.99.66.31

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 15:05:07.095318079 CET	63183	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:05:07.133047104 CET	53	63183	8.8.8.8	192.168.2.5
Nov 28, 2020 15:05:08.119956970 CET	60151	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:05:08.147207022 CET	53	60151	8.8.8.8	192.168.2.5
Nov 28, 2020 15:05:09.232023001 CET	56969	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:05:09.259229898 CET	53	56969	8.8.8.8	192.168.2.5
Nov 28, 2020 15:05:10.403655052 CET	55161	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:05:10.430695057 CET	53	55161	8.8.8.8	192.168.2.5
Nov 28, 2020 15:05:11.601398945 CET	54757	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:05:11.628647089 CET	53	54757	8.8.8.8	192.168.2.5
Nov 28, 2020 15:05:24.353724003 CET	49992	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:05:24.391411066 CET	53	49992	8.8.8.8	192.168.2.5
Nov 28, 2020 15:05:30.798348904 CET	60075	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:05:30.836570024 CET	53	60075	8.8.8.8	192.168.2.5
Nov 28, 2020 15:05:32.873336077 CET	55016	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:05:32.900485992 CET	53	55016	8.8.8.8	192.168.2.5
Nov 28, 2020 15:05:36.056870937 CET	64345	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:05:36.083870888 CET	53	64345	8.8.8.8	192.168.2.5
Nov 28, 2020 15:05:55.802947998 CET	57128	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:05:55.854155064 CET	53	57128	8.8.8.8	192.168.2.5
Nov 28, 2020 15:05:57.190603018 CET	54791	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:05:57.227457047 CET	53	54791	8.8.8.8	192.168.2.5
Nov 28, 2020 15:06:01.406568050 CET	50463	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:06:01.449820995 CET	53	50463	8.8.8.8	192.168.2.5
Nov 28, 2020 15:06:02.737278938 CET	50394	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:06:02.774029970 CET	53	50394	8.8.8.8	192.168.2.5
Nov 28, 2020 15:06:34.033473015 CET	58530	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:06:34.060530901 CET	53	58530	8.8.8.8	192.168.2.5
Nov 28, 2020 15:07:10.783339977 CET	53813	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:07:10.818804026 CET	53	53813	8.8.8.8	192.168.2.5
Nov 28, 2020 15:07:21.704451084 CET	63732	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:07:21.745177984 CET	53	63732	8.8.8.8	192.168.2.5
Nov 28, 2020 15:07:23.718533993 CET	57344	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:07:23.745588064 CET	53	57344	8.8.8.8	192.168.2.5
Nov 28, 2020 15:07:26.942025900 CET	54450	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:07:27.013183117 CET	53	54450	8.8.8.8	192.168.2.5
Nov 28, 2020 15:07:27.148013115 CET	59261	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:07:27.195842981 CET	53	59261	8.8.8.8	192.168.2.5
Nov 28, 2020 15:07:28.849608898 CET	57151	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:07:28.885410070 CET	53	57151	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 15:07:33.152123928 CET	59413	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:07:33.153711081 CET	60516	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:07:33.187537909 CET	53	59413	8.8.8.8	192.168.2.5
Nov 28, 2020 15:07:33.189069033 CET	53	60516	8.8.8.8	192.168.2.5
Nov 28, 2020 15:07:33.945458889 CET	51649	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:07:33.981333017 CET	53	51649	8.8.8.8	192.168.2.5
Nov 28, 2020 15:07:34.729815006 CET	65086	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:07:34.852657080 CET	53	65086	8.8.8.8	192.168.2.5
Nov 28, 2020 15:07:35.556140900 CET	56432	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:07:35.591646910 CET	53	56432	8.8.8.8	192.168.2.5
Nov 28, 2020 15:07:36.369559050 CET	52929	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:07:36.410165071 CET	53	52929	8.8.8.8	192.168.2.5
Nov 28, 2020 15:07:37.115530014 CET	64317	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:07:37.142649889 CET	53	64317	8.8.8.8	192.168.2.5
Nov 28, 2020 15:07:38.323499918 CET	62372	53	192.168.2.5	8.8.8.8
Nov 28, 2020 15:07:38.362081051 CET	53	62372	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 28, 2020 15:06:01.406568050 CET	192.168.2.5	8.8.8.8	0xc97b	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:10.783339977 CET	192.168.2.5	8.8.8.8	0x7e08	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:21.704451084 CET	192.168.2.5	8.8.8.8	0x301b	Standard query (0)	7553014bd6a4211b.xyz	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:26.942025900 CET	192.168.2.5	8.8.8.8	0x43f1	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:27.148013115 CET	192.168.2.5	8.8.8.8	0xff88	Standard query (0)	www.evograph.ro	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:28.849608898 CET	192.168.2.5	8.8.8.8	0x8e02	Standard query (0)	www.evograph.ro	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:33.152123928 CET	192.168.2.5	8.8.8.8	0x7481	Standard query (0)	7553014bd6a4211b.xyz	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:33.153711081 CET	192.168.2.5	8.8.8.8	0x504	Standard query (0)	7553014bd6a4211b.xyz	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:34.729815006 CET	192.168.2.5	8.8.8.8	0x686	Standard query (0)	trueaerned.com	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:36.369559050 CET	192.168.2.5	8.8.8.8	0x7f6b	Standard query (0)	jojo-soft.xyz	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:37.115530014 CET	192.168.2.5	8.8.8.8	0x4cea	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:38.323499918 CET	192.168.2.5	8.8.8.8	0x75f3	Standard query (0)	p421ls.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 28, 2020 15:06:01.449820995 CET	8.8.8.8	192.168.2.5	0xc97b	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 15:07:10.818804026 CET	8.8.8.8	192.168.2.5	0x7e08	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:21.745177984 CET	8.8.8.8	192.168.2.5	0x301b	No error (0)	7553014bd6a4211b.xyz		172.67.157.133	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:21.745177984 CET	8.8.8.8	192.168.2.5	0x301b	No error (0)	7553014bd6a4211b.xyz		104.24.114.254	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:21.745177984 CET	8.8.8.8	192.168.2.5	0x301b	No error (0)	7553014bd6a4211b.xyz		104.24.115.254	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:27.013183117 CET	8.8.8.8	192.168.2.5	0x43f1	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:27.195842981 CET	8.8.8.8	192.168.2.5	0xff88	No error (0)	www.evograph.ro	evograph.ro		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 15:07:27.195842981 CET	8.8.8.8	192.168.2.5	0xff88	No error (0)	evograph.ro		89.40.17.17	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 28, 2020 15:07:28.885410070 CET	8.8.8.8	192.168.2.5	0x8e02	No error (0)	www.evograph.ro	evograph.ro		CNAME (Canonical name)	IN (0x0001)
Nov 28, 2020 15:07:28.885410070 CET	8.8.8.8	192.168.2.5	0x8e02	No error (0)	evograph.ro		89.40.17.17	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:33.187537909 CET	8.8.8.8	192.168.2.5	0x7481	No error (0)	7553014bd6a4211b.xyz		172.67.157.133	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:33.187537909 CET	8.8.8.8	192.168.2.5	0x7481	No error (0)	7553014bd6a4211b.xyz		104.24.114.254	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:33.187537909 CET	8.8.8.8	192.168.2.5	0x7481	No error (0)	7553014bd6a4211b.xyz		104.24.115.254	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:33.189069033 CET	8.8.8.8	192.168.2.5	0x504	No error (0)	7553014bd6a4211b.xyz		172.67.157.133	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:33.189069033 CET	8.8.8.8	192.168.2.5	0x504	No error (0)	7553014bd6a4211b.xyz		104.24.114.254	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:33.189069033 CET	8.8.8.8	192.168.2.5	0x504	No error (0)	7553014bd6a4211b.xyz		104.24.115.254	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:34.852657080 CET	8.8.8.8	192.168.2.5	0x686	No error (0)	trueaerned.com		198.98.57.54	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:36.410165071 CET	8.8.8.8	192.168.2.5	0x7f6b	No error (0)	jojo-soft.xyz		104.31.72.130	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:36.410165071 CET	8.8.8.8	192.168.2.5	0x7f6b	No error (0)	jojo-soft.xyz		104.31.73.130	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:36.410165071 CET	8.8.8.8	192.168.2.5	0x7f6b	No error (0)	jojo-soft.xyz		172.67.194.188	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:37.142649889 CET	8.8.8.8	192.168.2.5	0x4cea	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:38.362081051 CET	8.8.8.8	192.168.2.5	0x75f3	No error (0)	p421ls.xyz		104.31.90.245	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:38.362081051 CET	8.8.8.8	192.168.2.5	0x75f3	No error (0)	p421ls.xyz		104.31.91.245	A (IP address)	IN (0x0001)
Nov 28, 2020 15:07:38.362081051 CET	8.8.8.8	192.168.2.5	0x75f3	No error (0)	p421ls.xyz		172.67.160.131	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- https:
  - 101.36.107.74

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49732	101.36.107.74	80	C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe

Timestamp	kBytes transferred	Direction	Data
Nov 28, 2020 15:07:10.385420084 CET	4381	OUT	GET /seemorebty/il.php?e=jg2_2qua HTTP/1.1 Connection: Keep-Alive Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image webp,image apng, q=0.8,application signed-exchange v=b3 Accept-Language: en-US,en;q=0.9 Referer: https://www.facebook.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit 537.36 (KHTML, like Gecko) Chrome 70.0.3538. 110 Safari 537.36 Host: 101.36.107.74

Timestamp	kBytes transferred	Direction	Data
Nov 28, 2020 15:07:10.647347927 CET	4381	IN	HTTP/1.1 200 OK Date: Sat, 28 Nov 2020 14:07:10 GMT Server: Apache/2.4.37 (centos) X-Powered-By: PHP/7.2.24 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 31 61 0d 0a 68 74 74 70 73 3a 2f 2f 69 70 6c 6f 67 67 65 72 2e 6f 72 67 2f 5a 64 6e 59 37 0d 0a 30 0d 0a 0d 0a Data Ascii: 1ahttps://iplogger.org/ZdnY70

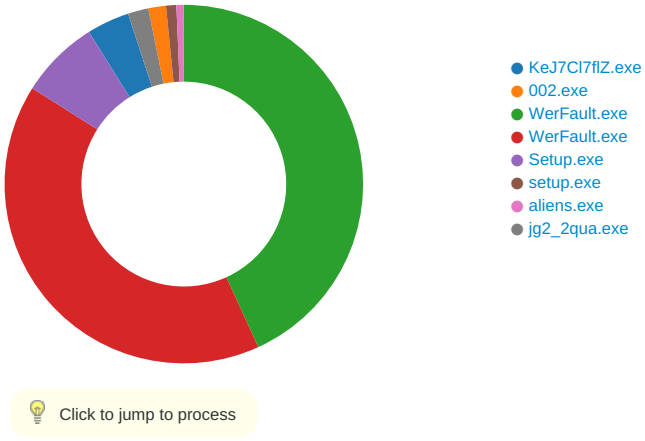
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 28, 2020 15:07:10.876172066 CET	88.99.66.31	443	192.168.2.5	49733	CN=*.iplogger.org CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Nov 20 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Nov 21 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Nov 28, 2020 15:07:27.068033934 CET	88.99.66.31	443	192.168.2.5	49737	CN=*.iplogger.org CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Nov 20 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Nov 21 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: KeJ7Cl7flZ.exe PID: 4576 Parent PID: 5700

General

Start time:	15:05:13
Start date:	28/11/2020
Path:	C:\Users\user\Desktop\KeJ7Cl7flZ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\KeJ7Cl7flZ.exe'
Imagebase:	0xec0000
File size:	7922731 bytes
MD5 hash:	4E759849412063C6590936671CE4AA0E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EC25E3	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EC25E3	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EC25E3	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EC25E3	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EC25E3	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\RarSFX0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	EC25E3	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\RarSFX0__tmp_rar_sfx_access_check_4900203	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	EC1C5C	CreateFileW
C:\Users\user\AppData\Local\Temp\RarSFX0\002.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EC1C5C	CreateFileW
C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EC1C5C	CreateFileW
C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EC1C5C	CreateFileW
C:\Users\user\AppData\Local\Temp\RarSFX0\file1.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EC1C5C	CreateFileW
C:\Users\user\AppData\Local\Temp\RarSFX0\BTRSetp.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EC1C5C	CreateFileW
C:\Users\user\AppData\Local\Temp\RarSFX0\askinstall21.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EC1C5C	CreateFileW
C:\Users\user\AppData\Local\Temp\RarSFX0\hjjgaa.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EC1C5C	CreateFileW
C:\Users\user\AppData\Local\Temp\RarSFX0\John_Ship.url	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EC1C5C	CreateFileW
C:\Users\user\AppData\Local\Temp\RarSFX0\ubisoftpro.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EC1C5C	CreateFileW
C:\Users\user\AppData\Local\Temp\RarSFX0\SSSS.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EC1C5C	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RarSFX0__tmp_rar_sfx_access_check_4900203	success or wait	1	EC24E4	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RarSFX0\002.exe	unknown	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 46 74 e6 02 02 15 88 51 02 15 88 51 02 15 88 51 9c b5 4f 51 03 15 88 51 df ea 46 51 0e 15 88 51 df ea 47 51 03 15 88 51 df ea 58 51 03 15 88 51 df ea 43 51 1f 15 88 51 02 15 89 51 31 17 88 51 44 44 57 51 1f 15 88 51 44 44 68 51 97 15 88 51 44 44 69 51 af 15 88 51 0f 47 6d 51 07 15 88 51 0f 47 53 51 03 15 88 51 02 15 1f 51 03 15 88 51 0f 47 56 51 03 15 88 51 52 69 63 68 02 15 88	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......Ft.....Q...Q...Q..OQ.. .Q..FQ...Q..GQ...Q..XQ...Q ..CQ ...Q...Q1..QDDWQ...QDDh Q...QDD iQ...Q.GmQ...Q.GSQ...Q... Q...Q.GVQ...QRich...	success or wait	20	EC235E	WriteFile
C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe	unknown	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 41 7b d1 6b 05 1a bf 38 05 1a bf 38 05 1a bf 38 0c 62 3c 38 06 1a bf 38 0c 62 2c 38 14 1a bf 38 05 1a be 38 a9 1a bf 38 1e 87 15 38 09 1a bf 38 1e 87 25 38 04 1a bf 38 1e 87 22 38 04 1a bf 38 52 69 63 68 05 1a bf 38 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 e4 e2 47 4f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 74 00 00 00 7a 07 00 00 42 00 00 af 38 00 00 00 10 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......A{.k...8...8...8.b<8.. .8.b,8...8...8...8...8...8..%8 ...8.."8...8Rich...8........PE ..L.....GO.................t.. .z...B...8.....	success or wait	65	EC235E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe	unknown	65536	4d 5a 40 00 01 00 00 00 02 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 57 69 6e 33 32 20 2e 45 58 45 2e 0d 0a 24 40 00 00 00 50 45 00 00 4c 01 03 00 ba 62 bc 5f 00 00 00 00 00 00 00 00 e0 00 03 03 0b 01 0e 10 00 72 0c 00 00 ec 04 00 00 00 00 00 e5 91 11 00 00 10 00 00 00 90 0c 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 60 13 00 00 02 00 00 00 00 00 00 02 00 00 81 00 00 10 00 00 70 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 90 11 00 e8 01 00 00 00 a0 11 00 5c be 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@........................... ....!..L.!Win32 .EXE...$ @...PE..L....b._.............. ...r........................@. ....`.... ....p............. ....\.....	success or wait	9	EC235E	WriteFile
C:\Users\user\AppData\Local\Temp\RarSFX0\file1.exe	unknown	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 13 9c fc f1 57 fd 92 a2 57 fd 92 a2 57 fd 92 a2 38 8b 39 a2 5e fd 92 a2 38 8b 0c a2 5e fd 92 a2 38 8b 38 a2 60 fd 92 a2 5e 85 01 a2 50 fd 92 a2 57 fd 93 a2 07 fd 92 a2 38 8b 3d a2 55 fd 92 a2 38 8b 08 a2 56 fd 92 a2 38 8b 0f a2 56 fd 92 a2 52 69 63 68 57 fd 92 a2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d2 6c b5 5f 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $...........W...W...W...8.9.^. ..8...^...8.8.`...^...P...W... ....8.=.U...8...V...8...V...Ri chW.......................... PE..L....l._...	success or wait	4	EC235E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RarSFX0\BTRSetp.exe	unknown	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 03 8f bd 5f 00 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 68 00 00 00 12 02 00 00 00 00 00 0a 00 03 00 00 60 01 00 00 20 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 03 00 00 04 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....h...............`... ....@.. ....@................	success or wait	3	EC235E	WriteFile
C:\Users\user\AppData\Local\Temp\RarSFX0\askinstall21.exe	unknown	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5f 09 a5 56 1b 68 cb 05 1b 68 cb 05 1b 68 cb 05 7e 0e c8 04 0b 68 cb 05 7e 0e ce 04 aa 68 cb 05 7e 0e cf 04 0c 68 cb 05 49 00 c8 04 0c 68 cb 05 49 00 ce 04 59 68 cb 05 49 00 cf 04 39 68 cb 05 7e 0e ca 04 0e 68 cb 05 1b 68 ca 05 d2 68 cb 05 89 01 c2 04 12 68 cb 05 89 01 34 05 1a 68 cb 05 1b 68 5c 05 1a 68 cb 05 89 01 c9 04 1a 68 cb 05 52 69 63 68 1b 68 cb 05 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $......._..V.h...h...h..~....h ..~....h..~....h..I....h..I... Yh..I...9h..~....h...h...h.... ...h....4..h...h\..h.......h.. Rich.h.........	success or wait	9	EC235E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RarSFX0\hjjgaa.exe	unknown	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 e4 45 65 d1 a0 24 0b 82 a0 24 0b 82 a0 24 0b 82 fb 4c 08 83 ad 24 0b 82 fb 4c 0e 83 0e 24 0b 82 fb 4c 0f 83 b6 24 0b 82 28 43 0f 83 b1 24 0b 82 28 43 08 83 b5 24 0b 82 28 43 0e 83 f1 24 0b 82 fb 4c 0a 83 a9 24 0b 82 a0 24 0a 82 df 24 0b 82 a1 49 02 83 a7 24 0b 82 a1 49 f4 82 a1 24 0b 82 a0 24 9c 82 a1 24 0b 82 a1 49 09 83 a1 24 0b 82 52 69 63 68 a0 24 0b 82 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........Ee..$...$...$...L...$ ...L...$...L...$..(C...$..(C.. .$..(C...$...L...$...$...$...I ...$...I...$...$...$...I...$.. Rich.$.........	success or wait	16	EC235E	WriteFile
C:\Users\user\AppData\Local\Temp\RarSFX0\John_Ship.url	unknown	117	5b 7b 30 30 30 32 31 34 41 30 2d 30 30 30 30 2d 30 30 30 30 2d 43 30 30 30 2d 30 30 30 30 30 30 30 30 30 30 34 36 7d 5d 0d 0a 50 72 6f 70 33 3d 31 39 2c 31 31 0d 0a 5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 74 5d 0d 0a 49 44 4c 69 73 74 3d 0d 0a 55 52 4c 3d 68 74 74 70 73 3a 2f 2f 69 70 6c 6f 67 67 65 72 2e 6f 72 67 2f 31 54 54 34 61 37 0d 0a	[{000214A0-0000-0000-C000-0000 00000046}]..Prop3=19,11..[Inte rnetShortcut]..IDList=..URL =ht tps://iplogger.org/1TT4a7..	success or wait	1	EC235E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RarSFX0\ubisoftpro.exe	unknown	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 e1 ed 26 69 a5 8c 48 3a a5 8c 48 3a a5 8c 48 3a d8 f5 a9 3a ba 8c 48 3a a8 de ac 3a a9 8c 48 3a ac f4 cc 3a a7 8c 48 3a ac f4 cb 3a a8 8c 48 3a ac f4 db 3a 8e 8c 48 3a a5 8c 49 3a 61 8e 48 3a e3 dd 97 3a 95 8c 48 3a e3 dd a8 3a ad 8d 48 3a e3 dd a9 3a 5b 8c 48 3a a8 de a9 3a a8 8c 48 3a a8 de 93 3a a4 8c 48 3a a8 de 96 3a a4 8c 48 3a 52 69 63 68 a5 8c 48 3a 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.........&i..H:..H:..H:...:.. H:...:..H:...:..H:...:..H:...: ..H:..l:a.H:...:..H:...:..H:...: [.H:...:..H:...:..H:...:..H: Rich..H:.......	success or wait	28	EC235E	WriteFile
C:\Users\user\AppData\Local\Temp\RarSFX0\SSSS.exe	unknown	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 af 65 6c 5d 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $............................. .... PE..L.....el]...	success or wait	5	EC235E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\KeJ7Cl7flZ.exe	unknown	8192	success or wait	1206	EC1D2C	ReadFile

Analysis Process: 002.exe PID: 3568 Parent PID: 4576

General

Start time:	15:05:15
Start date:	28/11/2020
Path:	C:\Users\user\AppData\Local\Temp\RarSFX0\002.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\RarSFX0\002.exe'
Imagebase:	0x1260000
File size:	1306112 bytes
MD5 hash:	6503C9C4F19A4B33B701CC5B97B349BC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RarSFX0\config.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	126267E	CreateFileA
C:\Users\user\AppData\Local\Google\Chrome\USERDA~1\Default\Login Data.bak	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	1000504F	CopyFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RarSFX0\config.ini	unknown	3	30 30 32	002	success or wait	1	12626C2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C.....................	success or wait	1	1000504F	CopyFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RarSFX0\config.ini	unknown	4096	success or wait	1	1008D57D	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\config.ini	unknown	4096	end of file	1	1008D57D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	0	100	success or wait	1	1001B343	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	0	4096	success or wait	1	1001B343	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	151552	success or wait	1	1008D57D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	1008D57D	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software	{c2bb7625-9318-a78a-103c-3f4b7 23d4137}	unicode	002	success or wait	1	1000E6A5	RegSetValueExA
HKEY_CURRENT_USER\Software	{a78b0a27-d469-f595-925f-db7cb5548136}	unicode	002	success or wait	1	1000E6A5	RegSetValueExA

Analysis Process: WerFault.exe PID: 204 Parent PID: 3568

General

Start time:	15:05:17
Start date:	28/11/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3568 -s 724
Imagebase:	0x2a0000

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:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDFCB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDFCB.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_002.exe_1c529646ab3c8a1fdb7fc485aa1d9d3291c12_6234ae00_0086ee01	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_002.exe_1c529646ab3c8a1fdb7fc485aa1d9d3291c12_6234ae00_0086ee01\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBF497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDFCB.tmp	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	success or wait	1	6DBF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	success or wait	1	6DBF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDFCB.tmp.xml	success or wait	1	6DBF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDFD8.tmp.csv	success or wait	1	6DBF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1FC.tmp.txt	success or wait	1	6DBF4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 b0 d7 c2 5f a4 05 12 00 00 00 00 00	MDMP..... ....._.....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.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 20 1d 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 f0 0d 00 00 ab d7 c2 5f 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 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... ...._.................. ....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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.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 4a a8 f5 00 00 00 00 00 d4 aa f5 00 00 00 00 00 d8 a6 5f e0 00 00 00 00 78 a7 f5 00 13 17 00 10 23 00 00 00 46 02 01 00 78 a7 f5 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+...J................._..... x.......#...F...x...+.........	success or wait	1	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	unknown	168	50 17 00 00 00 00 00 00 a5 01 00 c0 01 00 00 00 00 00 00 00 00 00 00 00 13 3b 0a 10 00 00 00 00 01 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 34 22 00 00	P.......................;.... ....4"..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	unknown	20	1d 00 00 00 00 30 ca 00 00 00 00 00 98 04 00 00 38 2f 00 00	.....0..........8/..	success or wait	29	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	unknown	1176	00 00 00 04 ff ff ff ff 00 00 26 01 a0 7b ad 77 58 18 4d 01 00 00 00 00 00 00 4d 01 a0 79 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 ea 74 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 00 00 f8 7b ad 77 ff ff ff ff 07 00 00 00 00 00 8a 7f 00 00 00 00 30 07 8a 7f 00 00 9a 7f 28 02 9b 7f 50 06 9c 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 80 9b 07 6d e8 ff ff 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 ad 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 02 00 00 00 06 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..........&..{.wX.M.......M..y .w..............t................ {.w................0....... (...P...................m........ ....`f.w.. ....PS.w.........B......	success or wait	28	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	unknown	256	8d 4d c0 e9 8e 19 f6 ff 8d 4d d8 e9 86 19 f6 ff 8b 54 24 08 8d 42 0c 8b 4a b8 33 c8 e8 f9 b7 fd ff 8b 4a fc 33 c8 e8 ef b7 fd ff b8 a4 ad 0c 10 e9 ae f6 fd ff 8d 4d d8 e9 59 19 f6 ff 8d 4d c0 e9 51 19 f6 ff 8b 54 24 08 8d 42 0c 8b 4a b4 33 c8 e8 c4 b7 fd ff 8b 4a fc 33 c8 e8 ba b7 fd ff b8 d8 ad 0c 10 e9 79 f6 fd ff 8d 8d cc fe ff ff e9 21 19 f6 ff 8d 8d 94 fe ff ff e9 fd 22 f6 ff 8b 54 24 08 8d 42 0c 8b 8a 6c fe ff ff 33 c8 e8 86 b7 fd ff 8b 4a fc 33 c8 e8 7c b7 fd ff b8 0c ae 0c 10 e9 3b f6 fd ff 8d 8d f0 e6 ff ff e9 e3 18 f6 ff 8d 8d 88 e7 ff ff e9 d8 18 f6 ff 8d 8d d0 e7 ff ff e9 cd 18 f6 ff 8d 8d b8 e7 ff ff e9 c2 18 f6 ff 8d 8d a0 e7 ff ff e9 b7 18 f6 ff 8d 8d 70 e7 ff ff e9 ac 18 f6 ff 8d 8d 08 e7 ff ff e9 a1 18 f6 ff ff b5 b0 e6 ff ff e8 5d 38 f7	.M.......M.......T$..B..J.3.......J.3.................M..Y....M..Q....T$..B..J.3.......J.3............y..........!...........".. T$..B...I...3.......J.3..|.........;...p.......................]8.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 9a f5 00 bc 9a a2 77 23 00 00 00 16 02 00 00 c0 99 f5 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?..+...S...+...+.................................w#...........+..	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	unknown	48	d0 17 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 c0 ca 00 00 00 00 00 44 f6 4a 01 00 00 00 00 bc 09 00 00 d0 65 00 00 cc 02 00 00 98 2a 00 00	....D.J........e.......*..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	unknown	4	2d 00 00 00	-...	success or wait	45	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	unknown	20	0e 00 00 00 30 00 30 00 32 00 2e 00 65 00 78 00 65 00 00 00	....0.0.2...e.x.e...	success or wait	45	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	unknown	752	00 00 7d 73 00 00 00 00 00 90 02 00 86 ea 02 00 ad 9a 47 32 18 22 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 01 00 00 00 00 00 00 00 00 00 00 00 00 00 24 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 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 90 74 02 00 00 00 00 00 20 bd 02 00 00 00 00 bc 4c 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 e3 69 03 00 00 00 00 00 e3 69 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8d b6 13 00 00 00 00 00 b3 48 0c 00 00 00 00 00 40 ff 1f 00 00 00 00 00 cf 5a 0c 00 00 00 00	..}s.....G2."..... .....B.....B?..... .....$..... ..@A.....Zb..... ....t..... ..... .L.....i.....i .....H..... @.....Z.....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	unknown	10448	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	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD78B.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 00 13 00 00 9c 07 00 00 05 00 00 00 d4 01 00 00 64 2d 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 80 1c 00 00 fc e7 00 00 15 00 00 00 ec 01 00 00 9c 1a 00 00 16 00 00 00 98 00 00 00 88 1c 00 00	.....d-.....T.....8.....T.....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 35 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.5.6.8.<./.P.i.d.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 30 00 30 00 32 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.>.0.0.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 32 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.>.0.0.0.0.0.0.0.0.2.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 39 00 39 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.>.4.9.9.3.<./.U.p.t.i.m.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 38 00 37 00 32 00 35 00 38 00 38 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.>.9.8.7.2.5.8.8.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 38 00 37 00 31 00 37 00 36 00 39 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.>.9.8.7.1.7.6.9.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 35 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.3.1.5.3.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 38 00 30 00 38 00 37 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.1.8.0.8.7.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 38 00 30 00 30 00 35 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.>.1.1.8.0.0.5.7.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 35 00 31 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.5.1.4.4.<./.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 35 00 31 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.5.1.4.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 35 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 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.>.3.6.5.0.4.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 32 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.6.2.3.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 34 00 32 00 32 00 32 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.>.4.2.2.2.9.7.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 34 00 34 00 35 00 36 00 34 00 34 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.>.4.4.5.6.4.4.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 34 00 32 00 32 00 32 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.>.4.2.2.2.9.7.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 35 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.5.7.6.<./.P.i.d.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 4b 00 65 00 4a 00 37 00 43 00 6c 00 37 00 66 00 6c 00 5a 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.>.K.e.J.7.C.l.7.f.l.Z...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 34 00 39 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.>.8.4.9.5.<./.U.p.t.i.m.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 38 00 32 00 35 00 38 00 37 00 33 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.>.1.8.2.5.8.7.3.9.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 38 00 32 00 34 00 39 00 33 00 31 00 38 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.>.1.8.2.4.9.3.1.8.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 35 00 33 00 31 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.3.1.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 39 00 31 00 31 00 31 00 39 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.>.1.9.1.1.1.9.3.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 39 00 31 00 31 00 31 00 39 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.>.1.9.1.1.1.9.3.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 36 00 33 00 37 00 34 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.>.2.6.3.7.4.4.<./.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 36 00 33 00 35 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.>.2.6.3.5.6.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 30 00 33 00 32 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.>.2.0.3.2.0.<./.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 31 00 39 00 37 00 36 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.>.1.9.7.6.0.<./.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 35 00 32 00 31 00 30 00 31 00 31 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.>.5.2.1.0.1.1.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 35 00 32 00 31 00 30 00 31 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.>.5.2.1.0.1.1.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 35 00 32 00 31 00 30 00 31 00 31 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.>.5.2.1.0.1.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	64	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 30 00 30 00 32 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.>.0.0.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 76 00 78 00 6c 00 6f 00 62 00 71 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.>.v.x.l.o.b.q.,. .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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 76 00 78 00 6c 00 6f 00 62 00 71 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.>.v.x.l.o.b.q.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 36 00 36 00 33 00 38 00 35 00 33 00 36 00 33 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.>.1.5.6.6.3.8.5.3.6.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 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.<./.F.l.a.g.s.>.	success or wait	3	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 30 00 2d 00 31 00 31 00 2d 00 32 00 38 00 54 00 32 00 33 00 3a 00 30 00 35 00 3a 00 32 00 30 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.=.".2.0.2.0.-.1.1.-.2.8.T.2.3.:.0.5.:.2.0.Z.".>.	success or wait	1	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 34 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 35 00 36 00 38 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 35 00 30 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 35 00 30 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.4.0.". .P.I.D.=.".3.5.6.8.". .U.p.t.i.m.e.M.S.=.".7.5.0.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t. i.o.n.M.S.=.".7.5.0.". .S.u.s. p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 30 00 38 00 39 00 62 00 62 00 37 00 65 00 2d 00 64 00 61 00 66 00 33 00 2d 00 34 00 37 00 35 00 62 00 2d 00 38 00 65 00 39 00 62 00 2d 00 63 00 31 00 37 00 61 00 64 00 35 00 31 00 37 00 36 00 35 00 61 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.e.0.8.9.b.b.7.e.-.d.a.f.3.-.4.7.5.b.-.8.e.9.b.-.c.1.7.a.d.5.1.7.6.5.a.b.<./.G.u.i.d.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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 30 00 2d 00 31 00 31 00 2d 00 32 00 38 00 54 00 32 00 33 00 3a 00 30 00 35 00 3a 00 32 00 30 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.>.2.0.2.0.-.1.1.-.2.8.T.2.3.:.0.5.:.2.0.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD97.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	6DBF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDFCB.tmp.xml	unknown	4632	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	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_002.exe_1c529646ab3c8a1fdb7fc485aa1d9d3291c12_6234ae00_0086ee01\Report.wer	unknown	2	ff fe	..	success or wait	1	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_002.exe_1c529646ab3c8a1fdb7fc485aa1d9d3291c12_6234ae00_0086ee01\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	176	6DBF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_002.exe_1c529646ab3c8a1fdb7fc485aa1d9d3291c12_6234ae00_0086ee01\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 39 00 32 00 39 00 39 00 33 00 37 00 32 00 30 00 37 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.9.2.9.9.3.7.2.0.7.	success or wait	1	6DBF497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DC136BF	unknown
\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DC136BF	unknown
\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea	success or wait	1	6DC136BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6DC11FB2	RegCreateKeyExW
\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DBF43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea	ProgramId	unicode	000602cdabd27f6c7dfbc5ad862c4027a30d00000408	success or wait	1	6DC136BF	unknown
\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea	FileId	unicode	0000fedb760f67f6000bf311c76dff55c35beeda8b81	success or wait	1	6DC136BF	unknown

<table>
<tr><th>Key Path</th><th>Name</th><th>Type</th><th>Data</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>LowerCaseLongPath</td><td>unicode</td><td>c:\users\user\appdata\local\temp\rarsfx0\002.exe</td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>LongPathHash</td><td>unicode</td><td>002.exe|29be74ea</td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>Name</td><td>unicode</td><td>002.exe</td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>Publisher</td><td>unicode</td><td>todo: <l..></td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>Version</td><td>unicode</td><td>1.0.0.1</td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>BinFileVersion</td><td>unicode</td><td>1.0.0.1</td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>BinaryType</td><td>unicode</td><td>pe32_i386</td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>ProductName</td><td>unicode</td><td>todo: <...></td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>ProductVersion</td><td>unicode</td><td>1.0.0.1</td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>LinkDate</td><td>unicode</td><td>11/09/2020 08:51:09</td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>BinProductVersion</td><td>unicode</td><td>1.0.0.1</td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>Size</td><td>B</td><td>00 EE 13 00 00 00 00 00</td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>Language</td><td>dword</td><td>2052</td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>IsPeFile</td><td>dword</td><td>1</td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>\REGISTRY\A\{38d36c03-1d8e-ebff-8bbe-9b421ec9af8c}\Root\InventoryApplicationFile\002.exe|29be74ea</td><td>IsOsComponent</td><td>dword</td><td>0</td><td>success or wait</td><td>1</td><td>6DC136BF</td><td>unknown</td></tr>
<tr><td>HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug</td><td>ExceptionRecord</td><td>binary</td><td>A5 01 00 C0 01 00 00 00 00 00 00 00 13 3B 0A 10 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>success or wait</td><td>1</td><td>6DC11FE8</td><td>RegSetValueExW</td></tr>
</table>

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 204 Parent PID: 3568

General

Start time:	15:05:27
Start date:	28/11/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3568 -s 740
Imagebase:	0x2a0000
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	6FE81717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD05.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD05.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_002.exe_566a661da143f3fc1b192bf169fbb3659a52956_6234ae00_00871c35	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_002.exe_566a661da143f3fc1b192bf169fbb3659a52956_6234ae00_00871c35\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FE7497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD05.tmp	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	success or wait	1	6FE74BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	success or wait	1	6FE74BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD05.tmp.xml	success or wait	1	6FE74BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD24.tmp.csv	success or wait	1	6FE74BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF77.tmp.txt	success or wait	1	6FE74BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 bb d7 c2 5f a4 05 12 00 00 00 00 00	MDMP..... ....._.....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.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 20 1d 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 f0 0d 00 00 ab d7 c2 5f 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 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... ...._.................. ....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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.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 4a a8 f5 00 00 00 00 00 d4 aa f5 00 00 00 00 00 d8 a6 5f e0 00 00 00 00 78 a7 f5 00 13 17 00 10 23 00 00 00 46 02 01 00 78 a7 f5 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+...J................._..... x.......#...F...x...+.........	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	unknown	168	50 17 00 00 00 00 00 05 00 00 c0 08 00 00 00 00 00 00 00 00 00 00 00 13 17 00 10 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 34 22 00 00	P............................. ....4"..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	unknown	20	1a 00 00 00 00 30 ca 00 00 00 00 00 98 04 00 00 08 2f 00 00	.....0.........../..	success or wait	26	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	unknown	1176	00 00 00 04 ff ff ff ff 00 00 26 01 a0 7b ad 77 58 18 4d 01 00 00 00 00 00 00 4d 01 a0 79 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 10 ea 74 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 00 00 f8 7b ad 77 ff ff ff ff 07 00 00 00 00 00 8a 7f 00 00 00 00 30 07 8a 7f 00 00 9a 7f 28 02 9b 7f 50 06 9c 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 80 9b 07 6d e8 ff ff 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 ad 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 ad 77 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 02 00 00 00 06 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..........&..{.wX.M.......M..y .w...............t................. {.w................0....... (...P...................m........ ....`f.w.. ....PS.w.........B......	success or wait	25	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	unknown	1168	bc b1 a2 77 d6 c9 a0 77 b4 00 00 00 aa aa aa aa 10 00 00 00 04 fc 1d 01 d0 fc 1d 01 aa aa aa aa 40 c7 a0 77 40 c7 a0 77 aa aa aa aa 00 90 ca 00 00 90 ca 00 00 00 00 00 b4 00 00 00 aa aa aa aa b4 00 00 00 aa aa aa aa 00 90 ca 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 e6 4d 01 00 00 00 00 00 00 00 00 98 6b 4d 01 00 30 ca 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 10 f7 4a 01 54 32 ca 00 18 f7 4a 01 08 70 4d 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..................... ..@..w@..w................... ....M... ....kM..0................. ....J.T2 ....J..pM....................	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.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 4a a8 f5 00 00 00 00 00 d4 aa f5 00 00 00 00 00 aa aa aa aa 00 00 00 00 78 a7 f5 00 13 17 00 10 23 00 00 00 46 02 01 00 78 a7 f5 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+...J...................... x.......#...F...x...+.........	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	unknown	48	d0 17 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 c0 ca 00 00 00 00 00 00 44 f6 4a 01 00 00 00 00 bc 09 00 00 a0 64 00 00 cc 02 00 00 98 2a 00 00	....D.J... ....d.......*..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	unknown	4	2d 00 00 00	-...	success or wait	45	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	unknown	20	0e 00 00 00 30 00 30 00 32 00 2e 00 65 00 78 00 65 00 00 00	....0.0.2...e.x.e...	success or wait	45	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	unknown	752	00 00 7d 73 00 00 00 00 00 90 02 00 86 ea 02 00 ad 9a 47 32 18 22 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 01 00 00 00 00 00 00 00 00 00 00 00 00 00 24 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 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 b0 5b 02 00 00 00 00 00 20 bd 02 00 00 00 00 09 56 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 fc 73 03 00 00 00 00 00 3b 79 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2c 56 1b 00 00 00 00 00 14 a9 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 cf 5a 0c 00 00 00 00	..}s.....G2."..... .....B.....B?..... .....$..... ..@A.....Zb..... ....[..... ..... .V.....s.....;y .....,V..... @.....Z.....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	unknown	10388	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 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 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	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER439.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 00 00 13 00 00 9c 07 00 00 05 00 00 00 a4 01 00 00 64 2d 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 58 1c 00 00 f8 d8 00 00 15 00 00 00 ec 01 00 00 9c 1a 00 00 16 00 00 00 98 00 00 00 88 1c 00 00	.....d-.....T.....8.....T.....X.....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 35 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.5.6.8.<./.P.i.d.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 30 00 30 00 32 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.>.0.0.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 32 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.>.0.0.0.0.0.0.0.0.2.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 36 00 34 00 36 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.>.1.6.4.6.1.<./.U.p.t.i.m.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 38 00 37 00 32 00 35 00 38 00 38 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.>.9.8.7.2.5.8.8.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 38 00 37 00 31 00 33 00 36 00 30 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.9.8.7.1.3.6.0.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 35 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.>.3.1.5.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 38 00 30 00 38 00 37 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.1.8.0.8.7.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 38 00 30 00 34 00 36 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.>.1.1.8.0.4.6.7.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 35 00 31 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.5.1.4.4.<./.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 35 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.5.1.3.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 38 00 36 00 39 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.>.3.8.6.9.6.<./.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 38 00 35 00 36 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.>.3.8.5.6.0.<./.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 34 00 32 00 32 00 32 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.>.4.2.2.2.9.7.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 34 00 34 00 35 00 36 00 34 00 34 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.>.4.4.5.6.4.4.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 34 00 32 00 32 00 32 00 32 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.>.4.2.2.2.9.7.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 35 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.5.7.6.<./.P.i.d.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 4b 00 65 00 4a 00 37 00 43 00 6c 00 37 00 66 00 6c 00 5a 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.>.K.e.J.7.C.l.7.f.l.Z...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 39 00 36 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.1.9.9.6.4.<./.U.p.t.i.m.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 38 00 32 00 35 00 38 00 37 00 33 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.>.1.8.2.5.8.7.3.9.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 38 00 32 00 34 00 39 00 33 00 31 00 38 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.>.1.8.2.4.9.3.1.8.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 35 00 33 00 31 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.3.1.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 39 00 31 00 31 00 31 00 39 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.>.1.9.1.1.1.9.3.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 39 00 31 00 31 00 31 00 39 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.>.1.9.1.1.1.9.3.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 36 00 33 00 37 00 34 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.>.2.6.3.7.4.4.<./.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 36 00 33 00 35 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.>.2.6.3.5.6.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 30 00 33 00 32 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.>.2.0.3.2.0.<./.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 31 00 39 00 37 00 36 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.>.1.9.7.6.0.<./.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 35 00 32 00 31 00 30 00 31 00 31 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.>.5.2.1.0.1.1.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 35 00 32 00 31 00 30 00 31 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.>.5.2.1.0.1.1.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 35 00 32 00 31 00 30 00 31 00 31 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.>.5.2.1.0.1.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	64	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 30 00 30 00 32 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.>.0.0.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 76 00 78 00 6c 00 6f 00 62 00 71 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.>.v.x.l.o.b.q.,. .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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 76 00 78 00 6c 00 6f 00 62 00 71 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.>.v.x.l.o.b.q.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 36 00 36 00 33 00 38 00 35 00 33 00 36 00 33 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.>.1.5.6.6.3.8.5.3.6.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.8.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 30 00 2d 00 31 00 31 00 2d 00 32 00 38 00 54 00 32 00 33 00 3a 00 30 00 35 00 3a 00 33 00 32 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.=.".2.0.2.0.-.1.1.-.2.8.T.2.3.:.0.5.:.3.2.Z.".>.	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 34 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 35 00 36 00 38 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 35 00 30 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 35 00 30 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.4.0.". .P.I.D.=.".3.5.6.8.". .U.p.t.i.m.e.M.S.=.".7.5.0.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t. i.o.n.M.S.=.".7.5.0.". .S.u.s. p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 62 00 62 00 30 00 37 00 63 00 64 00 33 00 2d 00 61 00 32 00 39 00 36 00 2d 00 34 00 64 00 38 00 63 00 2d 00 62 00 36 00 63 00 66 00 2d 00 62 00 35 00 63 00 61 00 38 00 37 00 38 00 38 00 36 00 65 00 31 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.2.b.b.0.7.c.d.3.-.a.2.9.6.-.4.d.8.c.-.b.6.c.f.-.b.5.c.a.8.7.8.8.6.e.1.b.<./.G.u.i.d.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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 30 00 2d 00 31 00 31 00 2d 00 32 00 38 00 54 00 32 00 33 00 3a 00 30 00 35 00 3a 00 33 00 32 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.>.2.0.2.0.-.1.1.-.2.8.T.2.3.:.0.5.:.3.2.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA45.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	6FE7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD05.tmp.xml	unknown	4628	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	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_002.exe_566a661da143f3fc1b192bf169fbb3659a52956_6234ae00_00871c35\Report.wer	unknown	2	ff fe	..	success or wait	1	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_002.exe_566a661da143f3fc1b192bf169fbb3659a52956_6234ae00_00871c35\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	176	6FE7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_002.exe_566a661da143f3fc1b192bf169fbb3659a52956_6234ae00_00871c35\Report.wer	unknown	42	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 35 00 38 00 39 00 30 00 32 00 30 00 32 00 32 00	M.e.t.a.d.a.t.a.H.a.s.h.=.5.8.9.0.2.0.2.2.	success or wait	1	6FE7497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{e62075af-6c47-e46b-9dca-c765c9fdde03}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6FE936BF	unknown
\REGISTRY\A\{e62075af-6c47-e46b-9dca-c765c9fdde03}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6FE936BF	unknown
\REGISTRY\A\{e62075af-6c47-e46b-9dca-c765c9fdde03}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6FE743D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	A5 01 00 C0 01 00 00 00 00 00 00 00 13 3B 0A 10 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 08 00 00 00 00 00 00 00 13 17 00 10 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6FE91FE8	RegSetValueExW

Analysis Process: Setup.exe PID: 6668 Parent PID: 4576

General

Start time:	15:05:40
Start date:	28/11/2020
Path:	C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe'
Imagebase:	0x400000
File size:	4240136 bytes
MD5 hash:	62EAEA103DD9BEB69E884F2EDE1ACD63
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40381F	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsq2FFC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405EEA	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsq2FFD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405EEA	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsq2FFD.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsq2FFD.tmp\Sibuia.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EA8	CreateFileW
C:\Users\user\AppData\Local\Temp\sib309A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FEE0EC5	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\sib309A.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6FEE1387	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\sib309A.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	6FEE1387	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\sib309A.tmp\SibCa.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FED197D	CreateFileW
C:\Users\user\AppData\Local\Temp\sib309A.tmp\SibClr.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FED197D	CreateFileW
C:\Users\user\AppData\Local\Temp\sib309A.tmp\0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6FEE1387	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\sib309A.tmp\0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6FEE1387	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\sib309A.tmp\0\setup.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FED197D	CreateFileW
C:\ProgramData\sib\{F9266136-0000-46F8-BC66-FDD9185E4296}	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object path not found	1	6FEE1387	CreateDirectoryW
C:\ProgramData\sib	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6FEE1387	CreateDirectoryW
C:\ProgramData\sib\{F9266136-0000-46F8-BC66-FDD9185E4296}	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6FEE1405	CreateDirectoryW
C:\ProgramData\sib\{F9266136-0000-46F8-BC66-FDD9185E4296}\sib.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FED197D	CreateFileW
C:\ProgramData\sib\{F9266136-0000-46F8-BC66-FDD9185E4296}\SibClr.dll	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6FEA570D	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\sib\{F9266136-0000-46F8-BC66-FDD9185E4296}\SibCa.dll	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6FEA5776	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Setup.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DA0C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsq2FFC.tmp	success or wait	1	403A6A	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsq2FFD.tmp	success or wait	1	406CEA	DeleteFileW
C:\Users\user\AppData\Local\Temp\sib309A.tmp	success or wait	1	6FEB149A	DeleteFileW
C:\Users\user\AppData\Local\Temp\sib309A.tmp\0\setup.exe	success or wait	1	6FEE11C6	DeleteFileW
C:\Users\user\AppData\Local\Temp\sib309A.tmp\SibCa.dll	success or wait	1	6FEE11C6	DeleteFileW
C:\Users\user\AppData\Local\Temp\sib309A.tmp\SibClr.dll	success or wait	1	6FEE11C6	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsq2FFD.tmp\Sibuia.dll	cannot delete	1	406E01	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsq2FFD.tmp\Sibuia.dll	unknown	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 41 de ae 2e 05 bf c0 7d 05 bf c0 7d 05 bf c0 7d 5e d7 c3 7c 0e bf c0 7d 93 d6 c5 7c 03 bf c0 7d 5e d7 c4 7c 1b bf c0 7d 5e d7 c5 7c bc bf c0 7d 5e d7 c6 7c 04 bf c0 7d 5e d7 c1 7c 24 bf c0 7d 05 bf c1 7d 78 bd c0 7d fd cf c4 7c 14 bf c0 7d fd cf c3 7c 12 bf c0 7d fd cf c5 7c 7a bf c0 7d b2 ce c9 7c 0a bf c0 7d b2 ce c0 7c 04 bf c0 7d b2 ce 3f 7d 04 bf c0 7d 05 bf 57 7d 04 bf c0	MZ......................@...... .... (...........!..L.!This program cannot be run in DOS mode.... $.......A......}...}...}^..\|.. .}...\|...}^..\|...}^..\|...}^..\| ...}^..\|$..}...}x..}...|...}.. .|...}...|z..}...|...}...|...} ..?}...}..W}...	success or wait	25	403505	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sib309A.tmp\SibCa.dll	unknown	4096	e1 b9 00 4d 5a 90 00 03 00 00 00 82 04 00 30 ff ff 00 00 b8 00 38 2d 01 10 40 04 38 19 30 80 00 70 0e 1f 00 ba 0e 00 b4 09 cd 21 b8 00 01 4c cd 21 54 68 69 73 00 20 70 72 6f 67 72 61 6d 00 20 63 61 6e 6e 6f 74 20 00 62 65 20 72 75 6e 20 69 00 6e 20 44 4f 53 20 6d 6f 80 64 65 2e 0d 0d 0a 24 04 b0 00 50 45 00 00 4c 01 03 00 10 64 38 32 bd 04 12 00 e0 00 00 02 21 0b 01 30 00 00 a6 a5 00 11 06 03 15 06 c4 00 07 20 00 03 42 e0 00 03 00 00 10 00 01 0b 02 0f 03 b7 01 11 01 bf 02 19 20 01 00 00 91 00 17 1e 2e 01 00 d7 40 85 01 2a fb 00 2d 00 1a 10 02 0a 01 23 00 09 01 06 02 03 60 b1 c3 00 00 4f 81 04 80 2b 68 07 01 84 82 0a 00 02 ae 00 00 28 1f 51 01 06 01 00 0c 00 03 14 80 13 38 57 01 07 a5 01 80 4f 08 88 15 08 80 07 48 41 88 07 2e 74 65 78 74 80 07 0c fe a4 00	...MZ.........0......8-..@.8.0 ..p.........!...L.!This. progr am. cannot .be run i.n DOS mo. de....$...PE..L....d82........ !..0............ ..B.................. ....@..*..-. .....#......`....O...+h.......... (.Q..........8W.....O...... HA...text......	success or wait	1	6FED1BB2	WriteFile
C:\Users\user\AppData\Local\Temp\sib309A.tmp\SibClr.dll	unknown	52520	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 64 38 32 bd 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 30 00 00 a6 00 00 00 06 00 00 00 00 00 00 06 c4 00 00 00 20 00 00 00 e0 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 1e 2e 01 00 03 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...d82........... .!..0................. ....@................	success or wait	1	6FED1BB2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sib309A.tmp\0\setup.exe	unknown	3956884	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 62 60 f7 f7 26 01 99 a4 26 01 99 a4 26 01 99 a4 92 9d 68 a4 2b 01 99 a4 92 9d 6a a4 ab 01 99 a4 92 9d 6b a4 3e 01 99 a4 b8 a1 5e a4 24 01 99 a4 1d 5f 9a a5 30 01 99 a4 1d 5f 9d a5 35 01 99 a4 1d 5f 9c a5 0a 01 99 a4 2f 79 1a a4 2c 01 99 a4 2f 79 0a a4 23 01 99 a4 26 01 98 a4 2c 00 99 a4 b1 5f 9c a5 17 01 99 a4 b1 5f 99 a5 27 01 99 a4 b4 5f 66 a4 27 01 99 a4 b1 5f 9b a5 27 01 99	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......b`..&...&...&.....h.+. ....j.......k.>.....^.$...._.. 0...._..5...._......./y..,.../y ..#...&...,...._......._..'... ._f.'...._..'..	success or wait	1	6FED1BB2	WriteFile
C:\ProgramData\sib\{F9266136-0000-46F8-BC66-FDD9185E4296}\sib.dat	unknown	1864	ff fe ff 26 7b 00 46 00 39 00 32 00 36 00 36 00 31 00 33 00 36 00 2d 00 32 00 43 00 45 00 32 00 2d 00 34 00 36 00 46 00 38 00 2d 00 42 00 43 00 36 00 36 00 2d 00 46 00 44 00 44 00 39 00 31 00 38 00 35 00 45 00 34 00 32 00 39 00 36 00 7d 00 ff fe ff 02 70 00 31 00 01 00 00 00 00 00 00 00 04 00 00 00 01 00 00 00 00 00 00 00 ff fe ff 05 61 00 64 00 6d 00 69 00 6e 00 ff fe ff 05 30 00 2e 00 30 00 2e 00 30 00 ff fe ff 00 ff fe ff 00 ff fe ff 12 49 00 3a 00 5c 00 6e 00 65 00 77 00 5f 00 6b 00 69 00 6c 00 6c 00 5c 00 70 00 31 00 5c 00 65 00 78 00 65 00 ff fe ff 09 70 00 31 00 28 00 33 00 29 00 2e 00 65 00 78 00 65 00 ff 45 01 7b 0a 20 20 20 20 22 61 70 70 56 65 72 73 69 6f 6e 22 3a 20 22 36 2e 30 2e 38 22 2c 0a 20 20 20 20 22 61 72 70 4e 6f 52 65 6d 6f 76 65 22	...&{.F.9.2.6.6.1.3.6.- .2.C.E.2.-.4.6.F.8.- .B.C.6.6.-.F.D.D. 9.1.8.5.E.4.2.9.6.}.....p.1... ....a.d.m.i. n.....0...0...0............I. :.\.n.e.w._.k.i.l.l.\.p.1.\.e. x.e.....p.1.(.3.)...e.x.e..E.{. "appVersion": "6.0.8",. "arpNoRemove"	success or wait	1	6FED1BB2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\sib\{F9266136-0000-46F8-BC66-FDD9185E4296}\SibClr.dll	0	52520	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 64 38 32 bd 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 30 00 00 a6 00 00 00 06 00 00 00 00 00 00 06 c4 00 00 00 20 00 00 00 e0 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 1e 2e 01 00 03 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L...d82..... .!..0..... ....@.....	success or wait	1	6FEA570D	CopyFileW
C:\ProgramData\sib\{F9266136-0000-46F8-BC66-FDD9185E4296}\SibCa.dll	0	4096	e1 b9 00 4d 5a 90 00 03 00 00 00 82 04 00 30 ff ff 00 00 b8 00 38 2d 01 10 40 04 38 19 30 80 00 70 0e 1f 00 ba 0e 00 b4 09 cd 21 b8 00 01 4c cd 21 54 68 69 73 00 20 70 72 6f 67 72 61 6d 00 20 63 61 6e 6e 6f 74 20 00 62 65 20 72 75 6e 20 69 00 6e 20 44 4f 53 20 6d 6f 80 64 65 2e 0d 0d 0a 24 04 b0 00 50 45 00 00 4c 01 03 00 10 64 38 32 bd 04 12 00 e0 00 00 02 21 0b 01 30 00 00 a6 a5 00 11 06 03 15 06 c4 00 07 20 00 03 42 e0 00 03 00 00 10 00 01 0b 02 0f 03 b7 01 11 01 bf 02 19 20 01 00 00 91 00 17 1e 2e 01 00 d7 40 85 01 2a fb 00 2d 00 1a 10 02 0a 01 23 00 09 01 06 02 03 60 b1 c3 00 00 4f 81 04 80 2b 68 07 01 84 82 0a 00 02 ae 00 00 28 1f 51 01 06 01 00 0c 00 03 14 80 13 38 57 01 07 a5 01 80 4f 08 88 15 08 80 07 48 41 88 07 2e 74 65 78 74 80 07 0c fe a4 00	...MZ.....0.....8-..@.8.0 ..p.....!...L.!This. progr am. cannot .be run i.n DOS mo. de....$...PE..L....d82..... !..0..... ..B..... .....@..*.-. .....#.....`....O...+h..... (.Q.....8W.....O..... HA...text.....	success or wait	1	6FEA5776	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Setup.exe.log	unknown	135	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 4a 53 63 72 69 70 74 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.Jscript, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	6DA0C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe	unknown	512	success or wait	200	403353	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe	unknown	4	success or wait	1	403353	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe	unknown	4	success or wait	1	403353	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe	unknown	8	success or wait	1	6FED19FE	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe	unknown	4096	success or wait	1	6FED19FE	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe	unknown	4096	success or wait	1	6FED19FE	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe	unknown	33822	success or wait	1	6FED19FE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D6D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D6D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D6303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D6DCA54	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\Setup.exe	unknown	3855010	success or wait	1	6FED19FE	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Users\user\AppData\Local\Temp\nsq2FFD.tmp\Sibuia.dll	success or wait	1	406CAB	MoveFileExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Users\user\AppData\Local\Temp\nsq2FFD.tmp\Sibuia.dll	\??\C:\Users\user\AppData\Local\Temp\nsq2FFD.tmp\Sibuia.dll \??\C:\Users\user\AppData\Local\Temp\nsq2FFD.tmp\	success or wait	1	406CAB	MoveFileExW

Analysis Process: setup.exe PID: 6732 Parent PID: 6668

General

Start time:	15:05:43
Start date:	28/11/2020
Path:	C:\Users\user\AppData\Local\Temp\sib309A.tmp\0\setup.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sib309A.tmp\0\setup.exe' -s
Imagebase:	0x50000

File size:	3956884 bytes
MD5 hash:	D64E3CC11AFC6331715BDFEC5F26C2A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5A174	CreateDirectoryW
C:\Program Files (x86)\ujvqkl7ofji6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5A174	CreateDirectoryW
C:\Program Files (x86)\ujvqkl7ofji6__tmp_rar_sfx_access_check_4929562	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5974C	CreateFileW
C:\Program Files (x86)\ujvqkl7ofji6\aliens.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5974C	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\ujvqkl7ofji6__tmp_rar_sfx_access_check_4929562	success or wait	1	5A084	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\ujvqkl7ofji6\aliens.exe	unknown	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 a8 9e 0c 00 00 a0 33 00 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2d 82 c1 ed 69 e3 af be 69 e3 af be 69 e3 af be d4 ac 39 be 6b e3 af be 60 9b 3a be 77 e3 af be 60 9b 2c be db e3 af be 60 9b 2b be 50 e3 af be 4e 25 c2 be 63 e3 af be 4e 25 d4 be 48 e3 af be 69 e3 ae be 64 e1 af be 60 9b 20 be 2f e3 af be 77 b1 3a be 6b e3 af be 77 b1 3b be 68 e3 af be 69 e3 38 be 68 e3 af be 60 9b 3e be 68 e3 af be 52 69 63 68 69 e3 af be 00 00 00 00 00 00 00	MZ......................@..... ....3.!This program cannot be run in DOS mode....$.......- ...i...i...i.....9.k. ..`.:.w...`.,.....`.+.P...N%.. c...N%..H...i...d...`. ./...w. :.k...w.;.h...i.8.h...`.>.h... Richi..........	success or wait	164	59EFE	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sib309A.tmp\0\setup.exe	unknown	8192	success or wait	74	5981C	ReadFile

Analysis Process: aliens.exe PID: 1112 Parent PID: 6732

General

Start time:	15:06:58
Start date:	28/11/2020
Path:	C:\Program Files (x86)\ujvqkl7ofji6\aliens.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\ujvqkl7ofji6\aliens.exe'
Imagebase:	0x400000
File size:	528498344 bytes
MD5 hash:	0F88FD9D557FFBE67A8897FB0FC08EE7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Ping_Command_in_EXE, Description: Detects an suspicious ping command execution in an executable, Source: 00000013.00000002.511085870.0000000003310000.00000040.00000001.sdmp, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\85F91A36E275562F.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	10020402	CopyFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\85F91A36E275562F.exe	0	1048576	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 a8 9e 0c 00 00 a0 33 00 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2d 82 c1 ed 69 e3 af be 69 e3 af be 69 e3 af be d4 ac 39 be 6b e3 af be 60 9b 3a be 77 e3 af be 60 9b 2c be db e3 af be 60 9b 2b be 50 e3 af be 4e 25 c2 be 63 e3 af be 4e 25 d4 be 48 e3 af be 69 e3 ae be 64 e1 af be 60 9b 20 be 2f e3 af be 77 b1 3a be 6b e3 af be 77 b1 3b be 68 e3 af be 69 e3 38 be 68 e3 af be 60 9b 3e be 68 e3 af be 52 69 63 68 69 e3 af be 00 00 00 00 00 00 00	MZ......................@..... ....3.!This program cannot be run in DOS mode....$.......- ...i...i...i.....9.k. ..`.:.w...`.,.....`.+.P...N%.. c...N%..H...i...d...`. ./...w. :.k...w.;.h...i.8.h...`.>.h... Richi..........	success or wait	392	10020402	CopyFileA
C:\Users\user\AppData\Local\Temp\85F91A36E275562F.exe	411041792	1048576	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	unknown	1	10020402	CopyFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\ujvqkl7ofji6\aliens.exe	unknown	77	success or wait	1	417410	ReadFile
C:\Program Files (x86)\ujvqkl7ofji6\aliens.exe	unknown	4210344	success or wait	1	4174E8	ReadFile

Analysis Process: jg2_2qua.exe PID: 5292 Parent PID: 4576

General

Start time:	15:07:08
Start date:	28/11/2020
Path:	C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\RarSFX0\jg2_2qua.exe'
Imagebase:	0x400000
File size:	574976 bytes
MD5 hash:	676757904C8383FD9ACBEED15AA8DCC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\VlcpVideoV1.0.1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40D123	CreateDirectoryW
C:\Users\user\Documents\VlcpVideoV1.0.1\jg2_2qua.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	40BCF8	CopyFileW
C:\Users\user\AppData\Local\Temp\RarSFX0\d	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4A99A5	CreateFileW
C:\Users\user\AppData\Local\Temp\RarSFX0\d	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40BBF6	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RarSFX0\d	success or wait	1	491254	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\VlcpVideoV1.0.1\jg2_2qua.exe	0	262144	4d 5a 40 00 01 00 00 00 02 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 57 69 6e 33 32 20 2e 45 58 45 2e 0d 0a 24 40 00 00 00 50 45 00 00 4c 01 03 00 ba 62 bc 5f 00 00 00 00 00 00 00 00 e0 00 03 03 0b 01 0e 10 00 72 0c 00 00 ec 04 00 00 00 00 00 e5 91 11 00 00 10 00 00 00 90 0c 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 13 00 00 02 00 00 00 00 00 00 02 00 00 81 00 00 10 00 00 70 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 90 11 00 e8 01 00 00 00 a0 11 00 5c be 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@........................... ....!..L.!Win32 .EXE...$ @...PE..L....b._.............. ...r........................@. ....`.... ....p.............. ....\.....	success or wait	3	40BCF8	CopyFileW
C:\Users\user\AppData\Local\Temp\RarSFX0\d	unknown	4096	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	4	49F08E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RarSFX0\d	unknown	4096	0a 00 00 00 01 0f eb 00 0f eb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	49F08E	WriteFile
C:\Users\user\AppData\Local\Temp\RarSFX0\d	unknown	26738688	2c 89 f0 1c ef cd ab 89 20 06 00 00 00 00 00 00 72 31 00 00 00 00 00 00 93 6c 7e 1b 1a 22 12 1b 06 77 4b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 20 02 67 00 0b 00 00 00 1d 2d 0e 1e 09 78 33 06 36 2d 0e 1e 09 78 5f 00 68 02 69 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 92 6b b1 5c 1a 22 12 1b 06 77 0d 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 59 00 00 00 0a 00 00 00 00 00 00 00 ee 42 00 00 00 00 00 00 14 00 00 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	,....... ....r1.......l~.." ...wK..................... .g......- ...x3.6-...x_.h.i....... ....k.\."...w.. ....Y............B.............	success or wait	1	40BC13	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	success or wait	5	4A00EA	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	unknown	4096	end of file	1	4A00EA	ReadFile
C:\Users\user\AppData\Local\Temp\RarSFX0\d	0	100	success or wait	4	41B145	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\ffdroider	success or wait	1	40B91D	RegCreateKeyW
HKEY_CURRENT_USER\Software\ffdroider\FFDroider	success or wait	1	40B91D	RegCreateKeyW

Disassembly

Code Analysis