ID: 671702
Sample Name: MIpuuSiSZ4.dll
Cookbook: default.jbs
Time: 14:09:07
Date: 22/07/2022
Version: 35.0.0 Citrine

Table of Contents

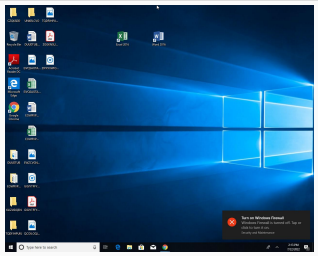
Windows Analysis Report

MIpuuSiSZ4.dll

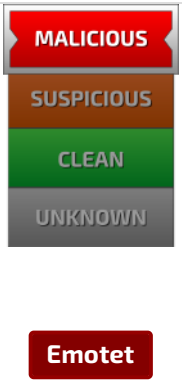
Overview

General Information

Sample Name:	MIpuuSiSZ4.dll
Analysis ID:	671702
MD5:	1dd34935a785a4.
SHA1:	c6c966e4ba623f…
SHA256:	8b5a10f9a8f2b25.
Tags:	exe OpenCTIBR Sandboxed
Infos:	



Detection



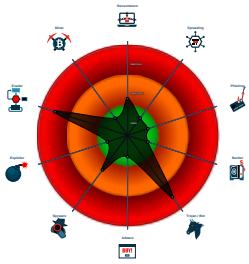
Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Changes security center settings (n…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Queries the volume information (nam…
- One or more processes crash
- Contains functionality to check if a d…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6740 cmdline: loaddll64.exe "C:\Users\user\Desktop\MIpuuSiSZ4.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6756 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\MIpuuSiSZ4.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6776 cmdline: rundll32.exe "C:\Users\user\Desktop\MIpuuSiSZ4.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 1992 cmdline: C:\Windows\system32\WerFault.exe -u -p 6776 -s 324 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - regsvr32.exe (PID: 6764 cmdline: regsvr32.exe /s C:\Users\user\Desktop\MIpuuSiSZ4.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 5660 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\GAjjZRZVj\QFdWkQKkPokX.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 6792 cmdline: rundll32.exe C:\Users\user\Desktop\MIpuuSiSZ4.dll,AddStroke MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 3660 cmdline: C:\Windows\system32\WerFault.exe -u -p 6792 -s 328 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - rundll32.exe (PID: 6836 cmdline: rundll32.exe C:\Users\user\Desktop\MIpuuSiSZ4.dll,AddWordsToWordList MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6852 cmdline: rundll32.exe C:\Users\user\Desktop\MIpuuSiSZ4.dll,AdviseInkChange MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 5852 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\ZcjkHmdxs\qpwRIlkrlFzB.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
- svchost.exe (PID: 6880 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6984 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 908 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6380 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1524 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 5112 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 1428 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 6256 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 6352 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 7100 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5604 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3308 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3052 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "101.69.85.108:20",
    "200.18.0.0:1",
    "208.9.0.0:2512",
    "82.10.0.0:2642",
    "144.1.49.1:2",
    "20.7.0.0:1",
    "176.6.0.0:1",
    "232.6.0.0:1",
    "136.6.0.0:1",
    "24.7.0.0:1",
    "248.6.0.0:1",
    "68.7.0.0:1",
    "80.7.0.0:1",
    "172.6.0.0:1",
    "96.7.0.0:1",
    "84.7.0.0:1",
    "4.7.0.0:1",
    "100.7.0.0:1",
    "112.7.0.0:1",
    "116.7.0.0:1",
    "180.6.0.0:1",
    "8.7.0.0:1",
    "236.6.0.0:1",
    "64.7.0.0:1",
    "204.6.0.0:1"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.364452628.0000015738060000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.345850399.0000000000710000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.351700174.0000020000071000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.662977936.0000000002D11000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000000.348541554.0000022FC4510000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.regsvr32.exe.710000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.0.rundll32.exe.22fc4510000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
12.2.regsvr32.exe.2cb0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.0.rundll32.exe.22fc4510000.3.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.0.rundll32.exe.14980010000.3.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 17 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 9 - Source IP: 192.168.2.7 - Destination IP: 174.138.33.49

Timestamp:	192.168.2.7174.138.33.494979470802404316 07/22/22-13:58:44.263207
SID:	2404316
Source Port:	49794
Destination Port:	7080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Lowering of HIPS / PFW / Operating System Security Settings

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information

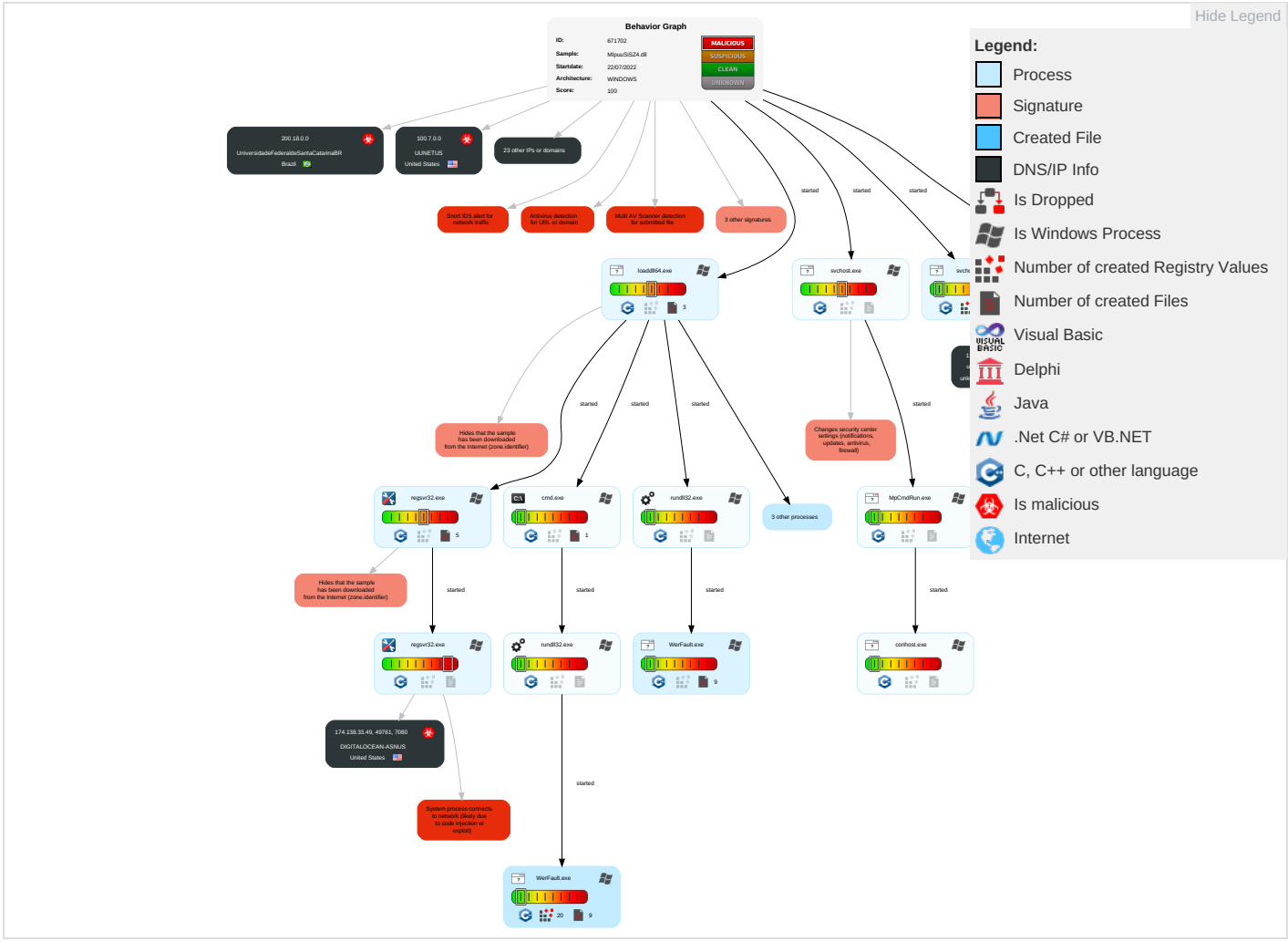
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	6 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Virtualization/Sandbox Evasion	Security Account Manager	3 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 System Service Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Regsvr32	Proc Filesystem	4 4 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Rundll32	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 DLL Side-Loading	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 File Deletion	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

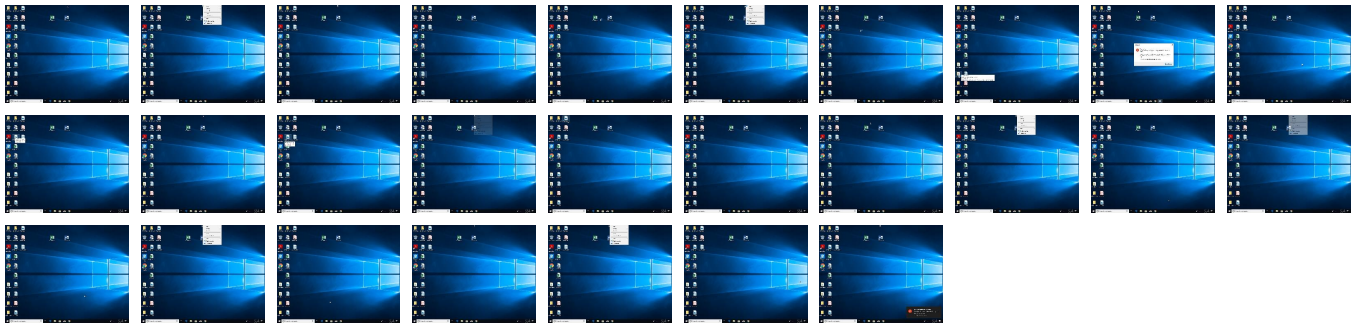
Behavior Graph



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
MIpuuSiSZ4.dll	72%	Virustotal		Browse
MIpuuSiSZ4.dll	54%	Metadefender		Browse
MIpuuSiSZ4.dll	88%	ReversingLabs	Win64.Trojan.Emotet	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://174.138.33.49/	0%	URL Reputation	safe	
http://https://174.138.33.49:7080/	0%	URL Reputation	safe	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://174.138.33.49:7080/x	100%	Avira URL Cloud	malware	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://174.138.33.49/T	100%	Avira URL Cloud	malware	
http://https://174.138.33.49:7080/tem	100%	URL Reputation	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://174.138.33.49:7080/944	100%	Avira URL Cloud	malware	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://%s.xboxlive.come	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

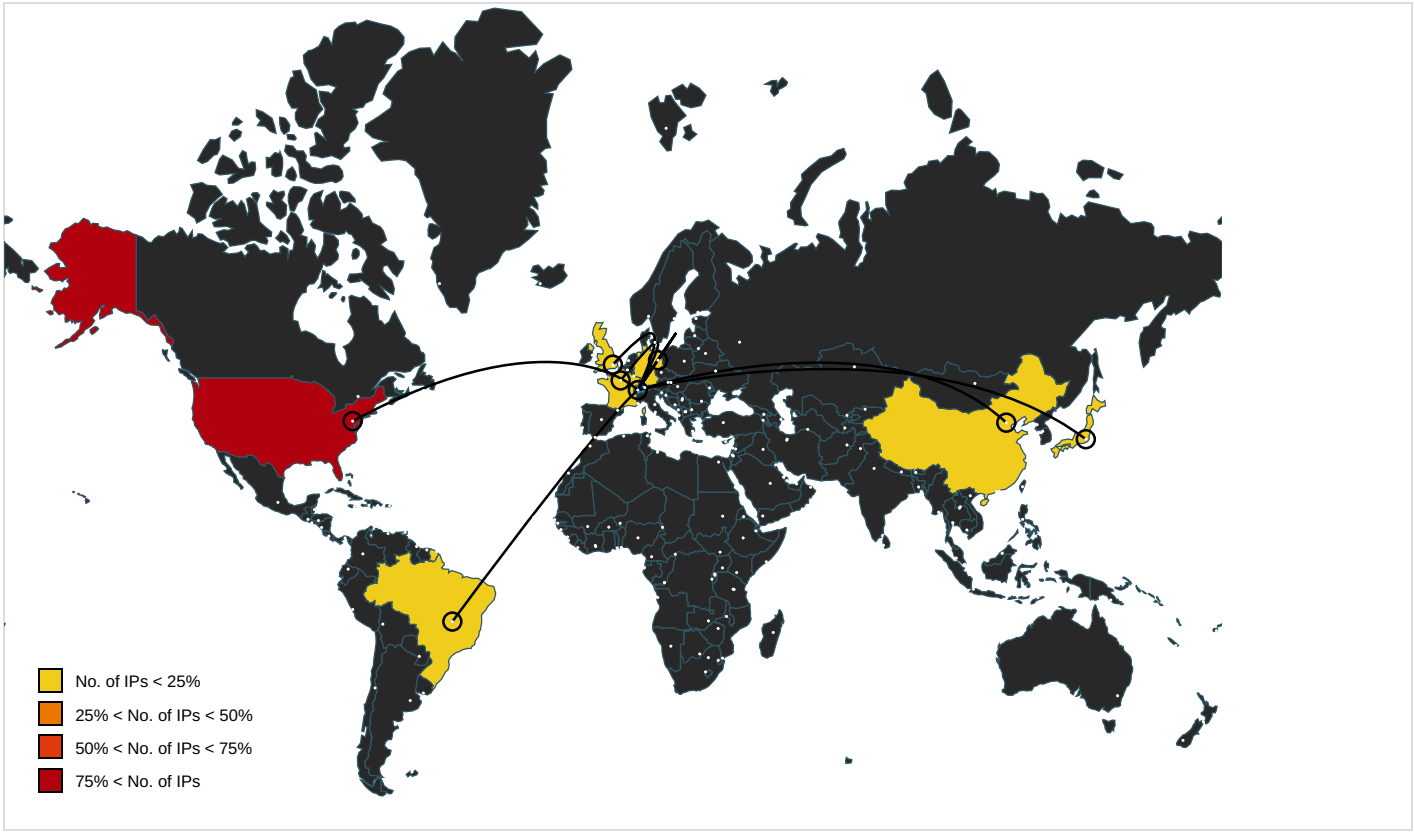
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000012.00000002.405452602.000002D97083D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000012.00000003.404914654.000002D970861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000012.00000002.405452602.000002D97083D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 00000012.00000002.405473479.000002D97085C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.404945537.000002D97085A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000012.00000002.405412295.000002D970813000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000012.00000003.404914654.000002D970861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000012.00000002.405457932.000002D970842000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.404980940.000002D970840000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.405017263.000002D970841000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000012.00000003.404914654.000002D970861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://174.138.33.49/	regsvr32.exe, 0000000C.00000002.661956267.0000000001301000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000C.00000003.444203872.0000000001301000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000012.00000003.404945537.000002D97085A000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000012.00000003.383087363.000002D970831000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000012.00000002.405457932.000002D970842000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.404980940.000002D970840000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.405017263.000002D970841000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://174.138.33.49:7080/	regsvr32.exe, 0000000C.00000002.661956267.0000000001301000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000C.00000002.661740445.00000000012D3000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000C.00000003.444163231.00000000012E2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000C.00000003.444203872.0000000001301000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000020.00000003.620490256.00000298A2781000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620519716.00000298A2C19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620333446.00000298A279D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620402747.00000298A2C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620475663.00000298A27AD000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620374463.00000298A27AD000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620430135.00000298A2C03000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000020.00000003.620490256.00000298A2781000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620519716.00000298A2C19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620333446.00000298A279D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620402747.00000298A2C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620475663.00000298A27AD000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620374463.00000298A27AD000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620430135.00000298A2C03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.bingmapsportal.com	svchost.exe, 00000012.00000002.405412295.000002D970813000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://174.138.33.49:7080/x	regsvr32.exe, 0000000C.00000002.661956267.0000000001301000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000C.00000003.444203872.0000000001301000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000012.00000002.405452602.000002D97083D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000012.00000003.404914654.000002D970861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000020.00000003.627116814.00000298A279A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://174.138.33.49/T	regsvr32.exe, 0000000C.00000002.661956267.0000000001301000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000C.00000003.444203872.0000000001301000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000012.00000003.404980940.000002D970840000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.405005326.000002D970845000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://174.138.33.49:7080/tem	regsvr32.exe, 0000000C.00000002.661740445.00000000012D3000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000C.00000003.444163231.00000000012E2000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000012.00000002.405452602.000002D97083D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000012.00000003.383087363.000002D970831000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.ver)	svchost.exe, 00000009.00000002.626913081.000002413A266000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000002.649749481.00000298A1EEA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000012.00000002.405473479.000002D97085C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.404980940.000002D970840000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.404945537.000002D97085A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000020.00000003.629383351.00000298A279F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000012.00000002.405412295.000002D970813000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.405452602.000002D97083D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000010.00000002.661987254.000002D0F6641000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000012.00000002.405466984.000002D97084E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.404854812.000002D970849000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000012.00000003.404914654.000002D970861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000012.00000003.383087363.000002D970831000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000012.00000003.404914654.000002D970861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.hotspotshield.com/	svchost.exe, 00000020.00000003.620490256.00000298A2781000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620519716.00000298A2C19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620333446.00000298A279D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620402747.00000298A2C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620475663.00000298A27AD000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620374463.00000298A27AD000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000020.00000003.620430135.00000298A2C03000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000012.00000002.405473479.000002D97085C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.404945537.000002D97085A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000020.00000003.627116814.00000298A279A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000012.00000002.405473479.000002D97085C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.404945537.000002D97085A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000012.00000003.404854812.000002D970849000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000012.00000003.404914654.000002D970861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://174.138.33.49:7080/944	regsvr32.exe, 0000000C.00000002.661740445.00000000012D3000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000C.00000003.444163231.00000000012E2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://disneyplus.com/legal.	svchost.exe, 00000020.00000003.627116814.00000298A279A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000012.00000003.383087363.000002D970831000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.405447191.000002D97083A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.come	svchost.exe, 00000010.00000002.661987254.000002D0F6641000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000012.00000003.404945537.000002D97085A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 00000010.00000002.661987254.000002D0F6641000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000012.00000003.404914654.000002D970861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://help.disneyplus.com.	svchost.exe, 00000020.00000003.627116814.00000298A279A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000010.00000002.661987254.000002D0F6641000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000012.00000002.405473479.000002D97085C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.404945537.000002D97085A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000012.00000003.404945537.000002D97085A000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
174.138.33.49	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
248.6.0.0	unknown	Reserved		unknown	unknown	true
20.7.0.0	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
101.69.85.108	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	true
176.6.0.0	unknown	Germany		12638	AS12638DuesseldorfDE	true
144.1.49.1	unknown	unknown		58541	CHINATELECOM-SHANDONG-QINGDAO-IDCQingdao266000CN	true
80.7.0.0	unknown	United Kingdom		5089	NTLGB	true
64.7.0.0	unknown	United States		4565	MEGAPATH2-US	true
24.7.0.0	unknown	United States		7922	COMCAST-7922US	true
112.7.0.0	unknown	China		24444	CMNET-V4SHANDONG-AS-APShandongMobileCommunicationCompany	true
4.7.0.0	unknown	United States		3356	LEVEL3US	true
208.9.0.0	unknown	United States		1239	SPRINTLINKUS	true
232.6.0.0	unknown	Reserved		unknown	unknown	true
96.7.0.0	unknown	United States		262589	INTERNEXABRASILOPERADORADETELECOMUNICACOESSABR	true
204.6.0.0	unknown	United States		174	COGENT-174US	true
172.6.0.0	unknown	United States		7018	ATT-INTERNET4US	true
100.7.0.0	unknown	United States		701	UUNETUS	true
180.6.0.0	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true
84.7.0.0	unknown	France		8228	CEGETEL-ASFR	true
200.18.0.0	unknown	Brazil		10715	UniversidadeFederaldeSantaCatarinaBR	true
136.6.0.0	unknown	United States		60311	ONEFMCH	true
236.6.0.0	unknown	Reserved		unknown	unknown	true
68.7.0.0	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
116.7.0.0	unknown	China		4809	CHINATELECOM-CORE-WAN-CN2ChinaTelecomNextGenerationCarr	true
8.7.0.0	unknown	United States		3356	LEVEL3US	true
82.10.0.0	unknown	United Kingdom		5089	NTLGB	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	671702
Start date and time: 22/07/202214:09:07	2022-07-22 14:09:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MIpuuSiSZ4.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	36
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.troj.evad.winDLL@33/16@0/28
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 86.9% (good quality ratio 81.6%) • Quality average: 75% • Quality standard deviation: 30.3%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Sleeps bigger than 300000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, WmiPrvSE.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.35.236.56, 93.184.221.240, 52.182.143.212, 20.189.173.21, 173.222.108.226, 173.222.108.210, 20.223.24.244
- Excluded domains from analysis (whitelisted): a767.dspw65.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu.azureedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, onedsblobprdcus15.centralus.cloudapp.azure.com, login.live.com, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, sls.update.microsoft.com, hlb.apr-52dd2-0.edgecastdns.net, onedsblobprdwus16.westus.cloudapp.azure.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, www.bing.com, fs.microsoft.com, wu.ec.azureedge.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior 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.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.chk

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.3593198815979092
Encrypted:	false
SSDEEP:	12:SnaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF318 0
Malicious:	false
Preview:	.....*.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....*..... ....

C:\ProgramData\Microsoft\Network\Downloader\edb.log

Process:	C:\Windows\System32\svchost.exe

File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.2494601363776735
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4Z:BJiRdwfu2SRU4Z
MD5:	70A5B7D8E2DEE8170DC1E083CCA3CE17
SHA1:	F3B8F17368F39ED7713E65721C93D6D3B7B9A2C2
SHA-256:	8D6AA38C684CD3C65C1F854E1B31676DD9E332B2134F06DF5BCCB0D91689F781
SHA-512:	A6C3D29A63E811A0CE4BEDD374CA271ED825E4FAA61B301FCE12B7BE26618BE99DAD311B4DCF521A304457744DDA18FFAE216563A93ABBC0B136C523F0D9AF1F
Malicious:	false
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....d#.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x9fe2e37f, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2505993140506313
Encrypted:	false
SSDEEP:	384:Ax9xz+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:An+SB2nSB2RSjlK/+mLesOj1J2
MD5:	19F8855F774735CCC8BCE5F79ED231B6
SHA1:	C105EA75CC9D92EBD60BF55AE5522FEE898489B9
SHA-256:	12C3290682DD6BB02DC0360DC3DA9575C5C400597D69DEECACE4DC70F99E5917
SHA-512:	E7EC65EB221DE16E577EAFE4E7174E4740786B50A210183903AC6751DABC1E2D85067CD8FDFD3FB02B44291F3CDA85AE105B74AC4103497BC935DA2091BD9301
Malicious:	false
Preview:	....e.f.3...w.....).....z..0....z..h.(.....z....).....3...w.....B.....@..... .....oXl0.....z.....`k.....z.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07550297560210162
Encrypted:	false
SSDEEP:	3:S+llJ7vVtulfwOGgAmmtOfyQllRB8ewll3VkttlmlnI:S+/Jr/ulAgAmYwhlRB8eQ3
MD5:	CD01E4F23E04035414BA9B9633F9F1EF
SHA1:	EFE4C001C27E9C473AC3A4B7C8471E215781E2A1
SHA-256:	DE5735C8E68FAA5BBB3AD2934EAB9B2E8103ACCF6E22179CDDC14081F9FE9558
SHA-512:	C2BDCD9E6EA1411D7D1E58D8961BF473FA39499F1633C61EAA357EE6CFCFF43E2174AC9704743176EF18DC4E9BC64BE47185C4B3C6A07C2AF594F347D8F6100
Malicious:	false
Preview:	..Lf.....3...w..0....z.....z.....z.....z...._.....z.u.....`k.....z.....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_MIp_773949b15a9dc27bfcd3f791ccbc8dda8da3511_ceeedb37_0e0d5ce9\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536

Entropy (8bit):	0.7738439296664732
Encrypted:	false
SSDEEP:	192:8pHrig1JKvHkhyJdJsj9U/u7s8S274ltN:wHriOKvkEJdJsjO/u7s8X4ltN
MD5:	7DC9F73DEF29002E1206FA23948F2E42
SHA1:	1514D0E4D04F00199CB62E657FE2EEA370DD278D
SHA-256:	A63786AA6434919A07EA05F40E5E86AEC6326D065C90A85C2F81BD5E2F0009B1
SHA-512:	E7E95D086D06B780D7C2121D3A3EC1812005AE0AE10E9E598A3AE2E9F82865D5AD004073569199730AAF6CBE21F997059B4363EBFBE2AB2C09A9BFC4B98E626 9
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.=.1.3.3.0.2.9.9.7.8.6.2.3.6.3.9.9.4.1.....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.=.1.3.3.0.2.9.9.7.8.6.7.0.6.7.1.0.8.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.4.f.d.1.8.f.3.-.2.0.b.a.-.4.f.f.0.-.b.8.5.1.-.e.6.d.5.0. c.c.5.7.e.9.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.a.b.d.5.e.7.7.-.0.1.0.e.-.4.3.a.4.-.9.b.0.c.-.e.9.2.b.6.9.3.7.f.a.a.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p. p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.M.I.p.u.u.S.i.S.Z.4...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.8.8.-.0.0.0.1.-. 0.0.1.d.-.2.f.2.5.-.c.1.7.2.0.f.9.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3. 4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_MIp_aa8bb9fdf8d32e2840ca8df43968d536d04b9a9_ceeedb37_07895910\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7729218762588249
Encrypted:	false
SSDEEP:	96:krgFa4QidJPnyEjT55I73f2pXIQcQqc620ycEBcw3pXaXz+HbHgSQgJPbmIDV9wR:ggOidJKgHkhyLtj9U/u7s8S274ltN3
MD5:	311D9D5DD757DFFCA2D4B6C46870D415
SHA1:	99417DC19B7ACFA4A69EEB8AAFAA08B956B455C4
SHA-256:	AFFA8D1168A1B8417E115A4B9C95BA8A68AD43287E0798545D518E72A72DFC1E
SHA-512:	2B8E6A134F98417A238288016E0F6B8D4073BEC251AC2589286FCAD00B2937F0523565819368C81CFB3EE1F047B0DD8426BB463976ECC14059179F0F0A89B1C5
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.=.1.3.3.0.2.9.9.7.8.6.0.1.1.9.1.7.1.3.....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.=.1.3.3.0.2.9.9.7.8.6.4.3.2.2.2.6.8.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.6.5.5.5.f.c.8.-.f.c.e.3.-.4.7.2.d.-.a.0.f.9.-.e.9.0.7.3. d.7.5.6.3.2.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.6.b.a.4.b.d.2.-.e.1.e.3.-.4.f.4.b.-.a.5.f.f.-.c.e.f.c.2.6.6.0.b.7.5.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p. p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.M.I.p.u.u.S.i.S.Z.4...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.7.8.-.0.0.0.1.-. 0.0.1.d.-.6.0.7.b.-.8.0.7.2.0.f.9.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3. 4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Jul 22 21:11:02 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	62478
Entropy (8bit):	2.362625578819154
Encrypted:	false
SSDEEP:	384:MQj1V4z7BXVjaYCr9x1lwdW4EaoO0w52SF8l:MQjz4xrCRxrqW4Ea7ZF6
MD5:	04E27A5A5CD926209E9DF3277BFD5568
SHA1:	B0F8A53B134CDCCB30E1950AE5DF92D52741CA2C
SHA-256:	1A3DF93B9CF4E8B649F71E40438CFD3D809684B16DB6C70BD278D4967FF7A39D
SHA-512:	8E5BA9B91ABABC7EE1363CA9D6E99DFD8ED770C4837FB56CCE3233AB27B9912CB6768FD3478F5CA487C29BDC0E5347F8D88ACD9917FAD162F55C609CCB985 C4C
Malicious:	false
Preview:	MDMP..... .....f..b.....h...8.....D...8:.....`.....8.....T.....0.....!.....#.....U.....B.....$$... ...Lw.....S...T.....x...;..b.....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...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..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Jul 22 21:11:04 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	64482
Entropy (8bit):	2.303579767806309

Encrypted:	false
SSDEEP:	384:DjWV4z7BXVjaaCmys8FqDMtlwdWke1EFfV6n+lk:DjI4xBC5q3e1EC
MD5:	B91B0DF6830BF2C08315A77C6D835667
SHA1:	E87AC87670539F0D814421700F853EA438EF304E
SHA-256:	8AD8C29581A4743FEF9C7C2772FB721797C5017052C86EF3EDB3368198D26345
SHA-512:	E0ACE2FBDFFA43B82BFE9DD19E652607248607D5C1BA457E41A85F6468797DE37E7DA2F3F704676D4255A2259518865E478413B43AB6995F47A89017A685F9A3
Malicious:	false
Preview:	MDMP..... .....h..b.....h...8.....D...8:.....`.....8.....T.....!.....#.....U.....B.....$$... ...Lw.....h.....T.....;..b.....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...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..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8748
Entropy (8bit):	3.6996177533951498
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNilDfCzG6Yx+Ygmf1RS/sCpr989bnhFhKfQtm:RrlsNiBfCS6YIYgmf1RSmnhFsf3
MD5:	76CC5955C86EA809660608C5BA848DAC
SHA1:	EDACA74055FDD4B7342A3ACEA1D0ECC7C76FE968
SHA-256:	F43D48F38CFECA62BAA7A6DF8C5563926432D4B4A754E320D6A219E829943282
SHA-512:	CBD881EC4AADF1D34AAE9991AFD750B7047515F28F000B3E6102EB8E7A3662DB5A34DD985E5974044ED7108AAB56CE6ED3DEC5415B86B604721B9A3F99BBE9 21
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.>.6.7.7. 6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAE.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4733
Entropy (8bit):	4.487431331312363
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtBI9LLWgc8sqYjws8fm8M4JC/WC/J8Frbyq85m/E7ZESC5Sh6d:uITfIN6grsqYURJ8bWb9+Vvh6d
MD5:	F022773265E899347C4417FE0AA02F68
SHA1:	DB1D3257D2301DFFF5014571A7DC99147CA3754F
SHA-256:	36AFA68F591F873B69550113030DE17EDC4B060E0F99CCBD34D9DC82D80E3EA5
SHA-512:	BA50C2B624639284BFD2351870F05BBBD28D2254857C123EC0E684C9687C941A6F7E91F59C1DB955712E357D1A0DD2BE2E79ED75D0545BD2DBBF0CF9F106D5 7
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="1614621" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8780
Entropy (8bit):	3.7010000674473056
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiPCyC86YUNC5LOgmf15S/3JPCprZ89bIYSfok4m:RrlsNi6yC86Y+C5LOgmf15SvJxItfo6
MD5:	E5C28F8EEFAB76EF6FD043E7608A16E4

SHA1:	32F14F79BEF26CC67FE114647893CC62A07A196D
SHA-256:	3C0CC2A7F21369758FF51B4B2C18961FB3041FC6129B15DF9401065054CAB076
SHA-512:	F9422786CB0A3018399FB284062E99C5043CCD5AAA980A887C365455816FE15B3E9A6D04CCFB0D108F4C3865F95ABC0DB8DC2C482AD386651FAF12CAC08862 5
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.>.6.7.9. 2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4675.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4733
Entropy (8bit):	4.487281289926747
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtBI9LLWgc8sqYjS8fm8M4JC/WC/JsFAqyq85m/EsTZESC5Sld:uITfIN6grsqYbJ8bU9vTVvld
MD5:	400AF3467BEA945FF08EEEEA48E212D4
SHA1:	0B3A96CCE356B960C83CBC001F9FB855441B408D
SHA-256:	D9870892CC9112382DBAD15D17931C7EC4CE4181B1F5237AA1F3C9B8F4BFDF88
SHA-512:	CC70BD271678E3EAA94366FB7F5940F59FCAB8B5BF4C395DC1D4FBD78DA8C4D174D8A619A3328715416501C50AA7A6C4FA9A1BA958F32ABDC4611FA38676D9 C9
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="1614621" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0- 11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E941 55B
Malicious:	false
Preview:	MSCF.....,.....I.....y.....Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C..... .`h!0.I.(C..1Q*L.p..".s..B.....H.....fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<.....3....s.T...._.'...%{v...s.....KgV.0..X=.A.9w9.Ea.x..... ...\.=.e.C2.....9.....`.o... .....@pm.. a.....-M.....{...s.mW.....;.+...A.....0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt.....h4.iQ?....[.K.....uI.....}.....d....M.....6q.Q~.0.\.'U^)`. .u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.l.E.6..a8.6..nq..x.r4..1t.....,.u.O..O.L...Uf...X.u.F .(.(.....".q...n{%U.-u....l6!....Z....~o0.}Q'.s.i ....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.135891594007862
Encrypted:	false
SSDEEP:	6:kKDu+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:6NkPlE99SNxAhUeE1
MD5:	393A75620FA9245A499CC73005C86D0E
SHA1:	556A243C5C445F94D53A27B455BB4C5997DA58B8
SHA-256:	074F48DB61AAE7BAE1D2CB0A71B962643B737A4B82A2EE57E3D1BA81C69F0937

SHA-512:	1BD9CD7B547AAC9F141E3BE355598CA09DA13A12318087C9B59E685E752BF01B0F7F3CD2264870457661378C507A14B3FFE58478EAAE2E0F494EE867E47D57E C
Malicious:	false
Preview:	p...... ....(.. ....L.........$..............h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.f.4.c.9.6.9.8.b.d.8.1.:.0."...

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA CA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.1630398757988987
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zEy+fs:j+s+v+b+P+m+0+Q+q+I+k
MD5:	79C0D9DDA6271582B2DD5E96FD072C8F
SHA1:	C6E2EFC633A02091186D2EEF6B6E6D9728BB8C20
SHA-256:	F0AAA959E0E482063E0A73C441F227AD4D89864BB1369BD9F04DCE2416064DBB
SHA-512:	985C3595CBC558823F96682BA09945350EEB386D76299E438F705099AC7ADADBACCBB1BC941C7A1C9041CBC4643416ACFB94362B7537D6109C6DD8B5EC9B48 5
Malicious:	false
Preview:	.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-.............-.

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	7.372720093100094
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	MIpuuSiSZ4.dll
File size:	850944
MD5:	1dd34935a785a419fb552b5086ea682e
SHA1:	c6c966e4ba623f9972273de07b842ffbb9a9efce
SHA256:	8b5a10f9a8f2b25057442111a01faf021ef7e048eab875a4078a44758d952c6f
SHA512:	79ab4a827fd581cd87fad4b0470bfcaf26f9471181c6c199706c54cc1b636cc7719306feac1b50c24d051f65c3b4d84bc662b8e33c03a1fced07f8023689dcfc
SSDEEP:	12288:jRCGXj4KVB9abMfyzfqvHWnyPv+LVHT2+2JNdX712kBjtOJZObrGzifb97Vw+Uvf:kGXj3X7FjkZqrqiBVwDbu5nP2F
TLSH:	7005D06773A509B5E0B7D139CA128E86FAB2BC091720F74B03E495752F23750A67F722

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d..t7..t7..t7w.w6..t7w.q6!.t7w.p6..t7..q6..t7..p6..t7..w6..t7w.u6..t7..u7..t7e.q6..t7e.t6..t7e..7..t7...7..t7e.v6..t7Rich..t

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180002c54
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	HIGH_ENTROPY_VA, NX_COMPAT
Time Stamp:	0x62CC7629 [Mon Jul 11 19:12:41 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	c2b03f92959f67ac494853faf0032582

Entrypoint Preview

Instruction
dec eax
mov dword ptr [esp+08h], ebx
dec eax
mov dword ptr [esp+10h], esi
push edi
dec eax
sub esp, 20h
dec ecx
mov edi, eax
mov ebx, edx
dec eax
mov esi, ecx
cmp edx, 01h
jne 00007FD5E8C48D07h
call 00007FD5E8C493BCh
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007FD5E8C48B70h

Instruction
int3
int3
int3
dec eax
and dword ptr [ecx+10h], 00000000h
dec eax
lea eax, dword ptr [0005B5E0h]
dec eax
mov dword ptr [ecx], eax
dec eax
mov eax, ecx
dec eax
mov dword ptr [ecx+08h], edx
ret
int3
inc eax
push ebx
dec eax
sub esp, 20h
dec eax
mov ebx, ecx
dec eax
mov eax, edx
dec eax
lea ecx, dword ptr [0005B591h]
xorps xmm0, xmm0
dec eax
mov dword ptr [ebx], ecx
dec eax
lea edx, dword ptr [ebx+08h]
dec eax
lea ecx, dword ptr [eax+08h]
movups dqword ptr [edx], xmm0
call 00007FD5E8C4AAD0h
dec eax
lea eax, dword ptr [0005B5A4h]
dec eax
mov dword ptr [ebx], eax
dec eax
mov eax, ebx
dec eax
add esp, 20h
pop ebx
ret
dec eax
and dword ptr [ecx+10h], 00000000h
dec eax
lea eax, dword ptr [0005B59Ch]
dec eax
mov dword ptr [ecx+08h], eax
dec eax
lea eax, dword ptr [0005B581h]
dec eax
mov dword ptr [ecx], eax
dec eax
mov eax, ecx
ret
int3
int3

Instruction
inc eax
push ebx
dec eax
sub esp, 20h
dec eax
mov ebx, ecx
dec eax
mov eax, edx
dec eax
lea ecx, dword ptr [0005B535h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x6eeb0	0x414	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6f2c4	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x79000	0x5b020	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x73000	0x4638	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd5000	0x80c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x687c0	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x687e0	0x138	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x5d000	0x338	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5b4c0	0x5b600	False	0.39445376624487005	data	6.495530086549807	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x5d000	0x12dae	0x12e00	False	0.39502276490066224	data	5.29311907790045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x70000	0x2740	0xe00	False	0.17606026785714285	data	2.4721317906474725	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x73000	0x4638	0x4800	False	0.5061848958333334	data	5.700987254121771	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
_RDATA	0x78000	0xf4	0x200	False	0.306640625	data	1.9910589321100538	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x79000	0x5b020	0x5b200	False	0.9233324759945131	data	7.923209381955667	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd5000	0x80c	0xa00	False	0.453515625	data	4.916763645477666	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_HTML	0x790a0	0x5ae00	data	English	United States
RT_MANIFEST	0xd3ea0	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	LockResource, CreateFileW, OutputDebugStringW, LoadResource, GetModuleFileNameW, VirtualAllocExNuma, WriteConsoleW, FindResourceA, GetCurrentProcess, CloseHandle, ReadConsoleW, ReadFile, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, GetModuleHandleW, RtlUnwindEx, RtlPcToFileHeader, RaiseException, InterlockedPushEntrySList, InterlockedFlushSList, GetLastError, SetLastError, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, EncodePointer, ExitProcess, GetModuleHandleExW, GetCurrentThread, HeapFree, HeapAlloc, GetStdHandle, GetFileType, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, MultiByteToWideChar, WideCharToMultiByte, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableW, FlsAlloc, FlsGetValue, FlsSetValue, FlsFree, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, GetProcessHeap, SetConsoleCtrlHandler, GetStringTypeW, GetFileSizeEx, SetFilePointerEx, SetStdHandle, HeapSize, HeapReAlloc, FlushFileBuffers, WriteFile, GetConsoleOutputCP, GetConsoleMode, RtlUnwind
USER32.dll	LoadStringW
ADVAPI32.dll	RegDeleteKeyW, RegCreateKeyExW, RegCloseKey, RegSetValueExW
ole32.dll	StringFromCLSID, CoTaskMemFree

Exports

Name	Ordinal	Address
AddStroke	2	0x180001744
AddWordsToWordList	3	0x180001970
AdviseInkChange	4	0x180001978
CloneContext	5	0x18000197c
CreateContext	6	0x180001984
CreateRecognizer	7	0x1800019ec
DestroyAlternate	8	0x180001a54
DestroyContext	9	0x180001a5c
DestroyRecognizer	10	0x180001ac4
DestroyWordList	11	0x180001ae8
DllRegisterServer	12	0x180001e0c
DllUnregisterServer	13	0x180001fc0
GetBestResultString	1	0x1800010b8
GetContextPreferenceFlags	14	0x18000201c
GetContextPropertyList	15	0x180002024
GetContextPropertyValue	16	0x18000202c
GetEnabledUnicodeRanges	17	0x180002034
GetGuide	18	0x18000203c
GetLatticePtr	19	0x180002080
GetLeftSeparator	20	0x1800022a4
GetPreferredPacketDescription	21	0x1800022ac
GetRecoAttributes	22	0x180002328
GetResultPropertyList	23	0x180002340
GetRightSeparator	24	0x180002348
GetUnicodeRanges	25	0x180002350
IsStringSupported	26	0x180002358
MakeWordList	27	0x180002360
Process	28	0x180002368
ResetContext	29	0x180002688
SetCACMode	30	0x1800026e0
SetContextPropertyValue	31	0x1800026e8
SetEnabledUnicodeRanges	32	0x1800026f0
SetFactoid	33	0x1800026f8
SetFlags	34	0x1800026fc
SetGuide	35	0x180002700
SetTextContext	36	0x1800027a8
SetWordList	37	0x1800027b0

Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

Snort IDS Alerts

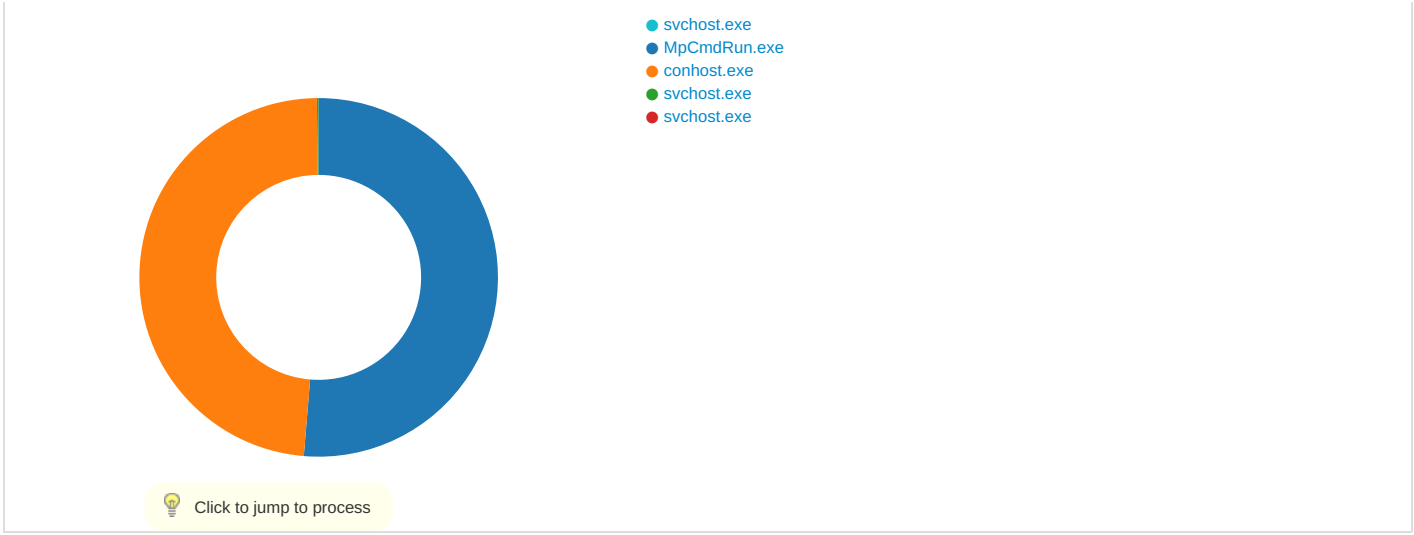
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.7174.138.33.49 4979470802404316 07/22/22-13:58:44.263207	TCP	2404316	ET CNC Feodo Tracker Reported CnC Server TCP group 9	49794	7080	192.168.2.7	174.138.33.49

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 22, 2022 14:11:39.982661963 CEST	49761	7080	192.168.2.3	174.138.33.49
Jul 22, 2022 14:11:40.086760998 CEST	7080	49761	174.138.33.49	192.168.2.3
Jul 22, 2022 14:11:40.086891890 CEST	49761	7080	192.168.2.3	174.138.33.49
Jul 22, 2022 14:11:40.112767935 CEST	49761	7080	192.168.2.3	174.138.33.49
Jul 22, 2022 14:11:40.215147972 CEST	7080	49761	174.138.33.49	192.168.2.3
Jul 22, 2022 14:11:40.233104944 CEST	7080	49761	174.138.33.49	192.168.2.3
Jul 22, 2022 14:11:40.233135939 CEST	7080	49761	174.138.33.49	192.168.2.3
Jul 22, 2022 14:11:40.233262062 CEST	49761	7080	192.168.2.3	174.138.33.49
Jul 22, 2022 14:11:42.999223948 CEST	49761	7080	192.168.2.3	174.138.33.49
Jul 22, 2022 14:11:43.104422092 CEST	7080	49761	174.138.33.49	192.168.2.3
Jul 22, 2022 14:11:43.105884075 CEST	49761	7080	192.168.2.3	174.138.33.49
Jul 22, 2022 14:11:43.111108065 CEST	49761	7080	192.168.2.3	174.138.33.49
Jul 22, 2022 14:11:43.250535965 CEST	7080	49761	174.138.33.49	192.168.2.3
Jul 22, 2022 14:11:43.646327019 CEST	7080	49761	174.138.33.49	192.168.2.3
Jul 22, 2022 14:11:43.648586035 CEST	49761	7080	192.168.2.3	174.138.33.49
Jul 22, 2022 14:11:46.647919893 CEST	7080	49761	174.138.33.49	192.168.2.3
Jul 22, 2022 14:11:46.647969007 CEST	7080	49761	174.138.33.49	192.168.2.3
Jul 22, 2022 14:11:46.648163080 CEST	49761	7080	192.168.2.3	174.138.33.49
Jul 22, 2022 14:13:29.858473063 CEST	49761	7080	192.168.2.3	174.138.33.49
Jul 22, 2022 14:13:29.858508110 CEST	49761	7080	192.168.2.3	174.138.33.49

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 6740, Parent PID: 6124

General

Target ID:	0
Start time:	14:10:18
Start date:	22/07/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\MIpuuSiSZ4.dll"
Imagebase:	0x7ff682600000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.364452628.0000015738060000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.364805521.0000015739971000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6756, Parent PID: 6740

General

Target ID:	1
Start time:	14:10:18
Start date:	22/07/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\MIpuuSiSZ4.dll",#1
Imagebase:	0x7ff689bc0000
File size:	273920 bytes

MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 6764, Parent PID: 6740

General

Target ID:	2
Start time:	14:10:19
Start date:	22/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\MIpuuSiSZ4.dll
Imagebase:	0x7ff6da7e0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.345850399.0000000000710000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.346021007.0000000002061000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\GAjjZRZVj\QFdWkQKkPokX.dll:Zone.Identifier	success or wait	1	207ED93	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6776, Parent PID: 6756

General

Target ID:	3
Start time:	14:10:19
Start date:	22/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\MIpuuSiSZ4.dll",#1
Imagebase:	0x7ff643150000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.348541554.0000022FC4510000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.377797661.0000022FC4510000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.348813253.0000022FC4571000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.338942505.0000022FC4510000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.377880147.0000022FC4571000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.338998123.0000022FC4571000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **6792**, Parent PID: **6740**

General

Target ID:	4
Start time:	14:10:19
Start date:	22/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\MIpuuSiSZ4.dll,AddStroke
Imagebase:	0x7ff643150000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.378702987.0000014980010000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.378747717.0000014980071000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.352241442.0000014980010000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.345097590.0000014980010000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.349632978.0000014980071000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.352325443.0000014980071000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **6836**, Parent PID: **6740**

General

Target ID:	5
Start time:	14:10:24
Start date:	22/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\MIpuuSiSZ4.dll,AddWordsToWordList
Imagebase:	0x7ff643150000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.351700174.0000020000071000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.351638703.0000020000010000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **6852**, Parent PID: **6740**

General	
Target ID:	6
Start time:	14:10:28
Start date:	22/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\MIpuuSiSZ4.dll,AdviseInkChange
Imagebase:	0x7ff643150000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.358968494.000001A029F41000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.358868561.000001A029EE0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: **6880**, Parent PID: **568**

General	
Target ID:	7
Start time:	14:10:30
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **6984**, Parent PID: **568**

General	
Target ID:	9
Start time:	14:10:45
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **5660**, Parent PID: **6764**

General

Target ID:	12
Start time:	14:10:54
Start date:	22/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\GAjjZRZVj\QFdWkQKkPokX.dll"
Imagebase:	0x7ff6da7e0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.662977936.0000000002D11000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.662715077.0000000002CB0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_3, Description: , Source: 0000000C.00000002.661348004.0000000001298000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **1992**, Parent PID: **6776**

General

Target ID:	13
Start time:	14:10:58
Start date:	22/07/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6776 -s 324
Imagebase:	0x7ff61dc30000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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	7FFC738E527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAE.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_MIp_aa8bb9fdf8d32e2840ca8df43968d536d04b9a9_ceeedb37_07895910	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_MIp_aa8bb9fdf8d32e2840ca8df43968d536d04b9a9_ceeedb37_07895910\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAE.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAE.tmp.xml	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9312.tmp.csv	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9381.tmp.txt	success or wait	1	7FFC738DE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 66 12 fd 62 fd 05 12 00 00 00 00 00	MDMP fb	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	9252	6	00 00 00 00 00 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	212	1420	09 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 24 24 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 fd fd 53 01 00 00 54 05 00 00 fd 03 00 00 78 1a 00 00 3b 12 fd 62 00 00 00 00 05 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 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	UB$$LwSTx;b0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	9976	1232	00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 15 43 fd 7f 00 00 00 00 00 00 00 00 00 00 fd 1b fd 2f 02 00 00 fd 57 0e fd fd 7f 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 06 02 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 00 08 fd 4b 29 fd 00 00 00 6e 00 0c 00 00 00 00 00 00 00 15 43 fd 7f 00 00 00 00 15 43 fd 7f 00 00 fd fd 4b 29 fd 00 00 00 10 fd 4b 29 fd 00 00 00 6e 00 0c 00 00 00 00 00 fd 00 0c 00 00 00 00 00 74 07 35 fd 2f 02 00 00 0a 00 00 00 00 00 00 00 17 02 00 30 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 74 07 35 fd 2f 02 00 00 fd 10 00 fd 01 00 00	C/W_3++S++K)nCCK)K) nt5/0t5/	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	1632	168	7c 1a 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 10 00 fd 01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 fd 26 00 00	|&	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	14904	20	54 00 00 00 64 fd 68 fd fd 7f 00 00 00 01 00 00 7c 3f 00 00	Tdh|?	success or wait	84	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	16252	256	57 00 00 00 fd 04 25 08 03 fd 7f 01 75 03 0f 05 fd fd 2e fd 0f 1f fd 00 00 00 00 00 4c fd 78 58 00 00 00 fd 04 25 08 03 fd 7f 01 75 03 0f 05 fd fd 2e fd 0f 1f fd 00 00 00 00 00 4c fd 78 59 00 00 00 fd 04 25 08 03 fd 7f 01 75 03 0f 05 fd fd 2e fd 0f 1f fd 00 00 00 00 00 fd fd fd fd 66 66 66 0f 1f fd 00 00 00 00 00 4c fd 78 5b 00 00 00 fd 04 25 08 03 fd 7f 01 75 03 0f 05 fd fd 2e fd 0f 1f fd 00 00 00 00 00 4c fd 78 5c 00 00 00 fd 04 25 08 03 fd 7f 01 75 03 0f 05 fd fd 2e fd 0f 1f fd 00 00 00 00 00 4c fd 78 5d 00 00 00 fd 04 25 08 03 fd 7f 01 75 03 0f 05 fd fd 2e fd 0f 1f fd 00 00 00 00 00 4c fd 78 5e 00 00 00 fd 04 25 08 03 fd 7f 01 75 03 0f 05 fd fd 2e fd 0f 1f fd 00 00 00 00 00 4c fd 78 5f 00 00 00 fd 04 25 08 03 fd 7f 01 75 03 0f	W%u.LX%u.LY%u.fffL[%u.L\%u.L]%u.L^%u.L_%u	success or wait	83	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	57058	256	48 fd fd 74 3d 48 fd 5c 24 08 57 48 fd fd 20 48 fd fd 48 fd fd 48 fd 1b 48 fd 4f 10 48 fd fd 74 05 fd fd 17 00 00 fd 18 00 00 00 48 fd fd fd 17 00 00 48 fd fd 75 fd 48 fd 5c 24 30 48 fd fd 20 5f fd fd 48 fd fd 48 fd 58 08 48 fd 68 10 48 fd 70 18 48 fd 78 20 41 54 41 56 41 57 48 fd fd 20 45 33 fd 4d fd fd 48 fd fd 48 fd fd 0f fd fd 00 00 00 48 fd fd 0f fd fd 00 00 00 48 fd 79 28 66 44 39 27 75 0a fd 32 02 04 fd fd 00 00 00 fd fd 00 00 00 48 fd fd fd 36 01 00 48 fd fd 4d fd fd 75 06 fd 2b 33 fd fd 6d 44 fd 33 4d 03 fd fd fd 48 03 fd 74 4e 48 fd fd 74 15 4c 3b fd 72 10 4c fd fd 48 fd fd 49 fd fd fd 2e 00 00 fd 34 4d fd fd 33 fd 49 fd fd fd 4d 35 00 00 48 fd fd 75 0d fd 29 01 00 fd 00 16 00 00 00 fd 10 4c 3b fd 73 10 fd 29 01 00 fd 00 22 00	Ht=H\$WH HHHHOHtHHuH\$0H _HHXHhHpHx ATAVAWH E3MHHHHy(fD9'u2H 6HMu+3mD3MHtNHtL;rLHI.4M3IM5Hu)L;s)"	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	11208	1232	fd fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 4b 29 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd 4b 29 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 68 fd 4b 29 fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 4b 29 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 68 fd fd 7f 00	3++S++FK)K)hK)K)h	success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	1900	48	fd 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 65 29 fd 00 00 00 18 fd 5b 29 fd 00 00 00 fd 03 00 00 7c 41 00 00 fd 04 00 00 68 35 00 00	e)[)|Ah5	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	9258	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	25	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	4556	4044	00 00 fd fd fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b fd 26 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 00 00 00 00 14 10 57 fd 2f 02 00 00 fd fd 59 fd 2f 02 00 00 00 00 57 fd 2f 02 00 00 3a 01 00 00 00 00 00 00 fd fd 75 fd fd 7f 00 00 fd fd 75 fd fd 7f 00 00 00 fd 59 fd 2f 02 00 00 fd 3c 20 fd 0f fd fd 01 14 10 57 fd 2f 02 00 00 fd fd 59 fd 2f 02 00 00 00 00 57 fd 2f 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 3a 01 00 00 00 00 00	<2|h+&BB?#`A pW/Y/W/:uuY/< W/Y/W/:	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	8608	644	01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 01 00 00 00 00 00 50 fd 02 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 00 00 00 01 00 00 00 7e fd 00 00 00 00 00 00 0c fd 03 00 00 00 00 00 43 5b 03 00 00 00 00 00 fd 0c 15 00 00 00 00 00 fd fd 0a 00 00 00 00 00 40 fd 1f 00 00 00 00 00 12 03 17 00 00 00 00 00 fd fd fd 4a 00 00 00 00 15 63 6e 1a 00 00 00 00 fd fd 59 21 00 00 00 00 01 5f fd 01 00 00 00 00 7f fd 00 00 45 16 01 00 00 fd 07 00 fd fd 07 00 fd fd 0a 00 4e 23 1a 00 12 03 17 00 16 fd 62 00 17 fd 01 00 56 56 1a 00 00 00 00 00 13 59 4b 00 fd 04 00 29 fd 00 00 00 00 00 00 00 00 00 00 11 13 00 00 2e 00 00 00 6d 01 00	ZbP~C[@JcnY!_EN#bVVYK).m	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	57314	5164	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 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 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 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	EventFileFile(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTim	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C2.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0a 00 00 fd 07 00 00 0d 00 00 00 68 0f 00 00 38 12 00 00 05 00 00 00 44 05 00 00 38 3a 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 30 0d 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 21 00 00 16 00 00 00 fd 00 00 00 fd 23 00 00	h8D8:`8T0!#	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2	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	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	84	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	<WERReportMetadata>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	128	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	<OSVersionInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	180	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	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	270	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	<Build>17134</Build>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	318	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	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	408	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	<Edition>Professional</Edition>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	478	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	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	620	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	<Revision>1</Revision>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	672	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	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	752	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	<Architecture>X64</Architecture>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	824	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	<LCID>1033</LCID>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	864	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	</OSVersionInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	916	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	<ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6776</Pid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 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	<ImageName>rundll32.exe</ImageName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1080	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	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 34 00 31 00 36 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>44166</Uptime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1230	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404"> 0</Wow64>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1316	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	<IptEnabled>0</IptEnabled>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1376	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	<ProcessVmInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1430	96	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 32 00 32 00 30 00 34 00 32 00 30 00 34 00 33 00 38 00 34 00 32 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2204204384256 </PeakVirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1536	80	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 32 00 32 00 30 00 33 00 34 00 30 00 39 00 31 00 30 00 30 00 38 00 30 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203409100800</VirtualSize>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1626	78	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 31 00 39 00 38 00 34 00 31 00 34 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	<PageFaultCount>198414</PageFaultCount>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1704	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1708	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1714	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 30 00 39 00 34 00 31 00 39 00 30 00 30 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	<PeakWorkingSetSize>709419008</PeakWorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1814	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1818	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1824	80	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 35 00 36 00 36 00 34 00 37 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>5664768</WorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1904	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1908	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	1914	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 30 00 37 00 36 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>107672</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2028	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2032	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2038	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 30 00 37 00 34 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>107472</QuotaPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2136	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2140	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2146	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 33 00 37 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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	<QuotaPeakNonPagedPoolUsage>23704</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2270	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2274	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2280	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 33 00 35 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	<QuotaNonPagedPoolUsage>23352</QuotaNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2388	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2392	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2398	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 36 00 36 00 37 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>2166784</PagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2474	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2478	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2484	96	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 30 00 32 00 38 00 30 00 37 00 38 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>80 2807808</ PeakPagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2580	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2584	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2590	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 36 00 36 00 37 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>2166784 </PrivateUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2662	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2666	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2670	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	</ProcessVmInformation >	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2716	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2720	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2724	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	<ParentProcess>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2754	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2758	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2764	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	<ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2804	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2808	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2816	30	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6756</Pid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2846	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2850	2	09 00		success or wait	4	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2858	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 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	<ImageName>cmd.exe</ImageName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	2930	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	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3032	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 34 00 36 00 30 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>44602</Uptime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3088	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3166	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3170	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3178	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	<IptEnabled>0</IptEnabled>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3230	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3234	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3242	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	<ProcessVmInformation>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3286	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3290	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3300	96	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 32 00 32 00 30 00 33 00 33 00 37 00 30 00 33 00 36 00 39 00 30 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2203370369024</PeakVirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3396	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3400	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3410	80	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 32 00 32 00 30 00 33 00 33 00 36 00 39 00 33 00 32 00 30 00 34 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203369320448</VirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3490	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3494	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3504	72	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 37 00 39 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>795</PageFaultCount>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3576	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3580	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3590	96	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 32 00 39 00 34 00 30 00 39 00 32 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	<PeakWorkingSetSize>2940928</PeakWorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3686	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3690	2	09 00		success or wait	5	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3700	80	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 32 00 39 00 32 00 38 00 36 00 34 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>2928640</WorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3780	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3784	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3794	112	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 37 00 38 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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	<QuotaPeakPagedPoolUsage>27840</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3906	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3910	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	3920	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 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 37 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 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	<QuotaPagedPoolUsage>27664</QuotaPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4016	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4020	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4030	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>4208</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4152	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4156	2	09 00		success or wait	5	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4166	106	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 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>3664</QuotaNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4272	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4276	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4286	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 39 00 37 00 31 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>2097152</PagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4376	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 35 00 33 00 39 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3153920</PeakPagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4468	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4472	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4482	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 39 00 37 00 31 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>2097152</PrivateUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4566	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	</ProcessVmInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4622	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	</ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4672	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	</ParentProcess>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4710	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	</ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4758	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	<ProblemSignatures>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4804	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	<EventType>APPCRASH</EventType>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	8	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	16	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	4874	104	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 5f 00 4d 00 49 00 70 00 75 00 75 00 53 00 69 00 53 00 5a 00 34 00 2e 00 64 00 6c 00 6c 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	<Parameter0>rundll32.exe_MIpuu SiSZ4.dll</Parameter0>	success or wait	8	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	5530	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	5534	2	09 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	5536	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	</ProblemSignatures>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	5576	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	5580	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	5582	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	<DynamicSignatures>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	5620	4	0d 00 0a 00		success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	5624	2	09 00		success or wait	12	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	5628	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	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6182	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6186	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6188	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	</DynamicSignatures>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6228	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6232	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6234	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	<SystemInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6272	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6276	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6280	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	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6374	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6378	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6382	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 62 00 61 00 68 00 72 00 63 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	<SystemManufacturer>vbahrc, Inc.</SystemManufacturer>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6488	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6492	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6496	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 62 00 61 00 68 00 72 00 63 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	<SystemProductName>vbahrc7,1</SystemProductName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6592	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6596	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6600	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 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 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	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6720	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6724	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6728	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 36 00 31 00 38 00 33 00 30 00 38 00 34 00 36 00 37 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	<OSInstallDate>1618308467</OSInstallDate>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6810	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6814	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6818	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	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6920	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6924	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6928	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 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	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7002	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	</SystemInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7042	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7046	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7048	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	<SecureBootState>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7082	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7086	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7090	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	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7186	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7190	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7192	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	</SecureBootState>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7228	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7232	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7234	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	<Integrator>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7258	4	0d 00 0a 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7262	2	09 00		success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7266	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 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7512	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7516	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7518	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	</Integrator>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7544	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7548	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7550	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 32 00 2d 00 30 00 37 00 2d 00 32 00 32 00 54 00 32 00 31 00 3a 00 31 00 31 00 3a 00 30 00 33 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-07-22T21:11:03Z">	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7650	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7654	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7658	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 39 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 37 00 37 00 36 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 33 00 33 00 30 00 37 00 38 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 33 00 33 00 30 00 37 00 38 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	<Process AsId="397" PID="6776" UptimeMS="33078" TimeSinceCreationMS="33078" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7924	4	0d 00 0a 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7928	2	09 00		success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	7934	196	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 34 00 31 00 31 00 32 00 33 00 38 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="4112384" TimelineUnitShift="12" Timeline="11111 11111"/>	success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8330	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8334	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8338	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8358	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8362	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8364	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	</ProcessTimelines>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8402	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8406	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8408	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	<ReportInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8446	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8450	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8454	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 36 00 35 00 35 00 35 00 66 00 63 00 38 00 2d 00 66 00 63 00 65 00 33 00 2d 00 34 00 37 00 32 00 64 00 2d 00 61 00 30 00 66 00 39 00 2d 00 65 00 39 00 30 00 37 00 33 00 64 00 37 00 35 00 36 00 33 00 32 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>76555fc8-fce3-472d-a0f9-e9073d756321</Guid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8552	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8556	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8560	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 32 00 2d 00 30 00 37 00 2d 00 32 00 32 00 54 00 32 00 31 00 3a 00 31 00 31 00 3a 00 30 00 33 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	<CreationTime>2022-07-22T21:11:03Z</CreationTime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8658	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8662	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8664	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	</ReportInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8704	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB9.tmp.WERInternalMetadata.xml	8708	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	</WERReportMetadata>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAE.tmp.xml	0	4733	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 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 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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_MIp_aa8bb9fdf8d32e2840ca8df43968d536d04b9a9_ceeedb37_07895910\Report.wer	0	2	fd fd		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_MIp_aa8bb9fdf8d32e2840ca8df43968d536d04b9a9_ceeedb37_07895910\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	150	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_MIp_aa8bb9fdf8d32e2840ca8df43968d536d04b9a9_ceeedb37_07895910\Report.wer	9436	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 36 00 36 00 33 00 32 00 30 00 34 00 37 00 31 00 32 00	MetadataHash=663204712	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC738DE3FE	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	FileId	unicode	00002f34ccfdd8141aeee2e89ffb070ce239c7d00706	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LowerCaseLongPath	unicode	c:\windows\system32\rundll32.exe	success or wait	1	7FFC73901D2D	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LongPathHash	unicode	rundll32.exe|c8d854bf61fafc41	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Name	unicode	rundll32.exe	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Publisher	unicode	microsoft corporation	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinFileVersion	unicode	10.0.17134.1	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinaryType	unicode	pe64_amd64	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductName	unicode	microsoft. windows. operating system	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductVersion	unicode	10.0.17134.1	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LinkDate	unicode	05/20/2093 18:03:41	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinProductVersion	unicode	10.0.17134.1	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Size	B	00 10 01 00 00 00 00 00	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Language	dword	1033	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsPeFile	dword	1	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsOsComponent	dword	1	success or wait	1	7FFC73901D2D	unknown

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\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 D0 3E AF DE FC 7F 00 00 01 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 F4 10 00 80 01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 96 00 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FFC739007CB	RegSetValueExW

Analysis Process: WerFault.exe PID: 3660, Parent PID: 6792

General

Target ID:	14
Start time:	14:11:00
Start date:	22/07/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6792 -s 328
Imagebase:	0x7ff61dc30000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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	7FFC738E527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4675.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4675.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_MIp_773949b15a9dc27bfcd3f791ccbc8dda8da3511_ceeedb37_0e0d5ce9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_MIp_773949b15a9dc27bfcd3f791ccbc8dda8da3511_ceeedb37_0e0d5ce9\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4675.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4675.tmp.xml	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER99FA.tmp.csv	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A2A.tmp.txt	success or wait	1	7FFC738DE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 68 12 fd 62 fd 05 12 00 00 00 00 00	MDMP hb	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	9252	6	00 00 00 00 00 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	212	1420	09 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 24 24 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 68 fd 01 02 00 00 54 05 00 00 fd 03 00 00 fd 1a 00 00 3b 12 fd 62 00 00 00 00 06 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00	UB$$LwhT;b0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	9976	1232	48 02 07 00 00 00 00 00 fd 0b 29 fd 49 01 00 00 3e 52 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 7f 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 fd 02 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 00 00 44 17 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 15 43 fd 7f 00 00 3e 52 fd fd 00 00 00 00 fd fd 27 2c 11 00 00 00 40 fd 27 2c 11 00 00 00 48 02 07 00 00 00 00 00 00 00 15 43 fd 7f 00 00 3e 52 fd fd 49 01 00 00 0a 00 00 00 00 00 00 00 fd 02 00 30 00 00 00 00 fd fd fd fd fd fd fd fd 51 fd fd 49 01 00 00 0a 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 fd 07 fd fd 49 01 00 00 fd 17 00 fd 01 00 00	H)I>R_3++S++DC>R',@' ,HC>RI0QII	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	1632	168	fd 1a 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 17 00 fd 01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c 02 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 fd 26 00 00	\&	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	14904	20	54 00 00 00 fd fd 37 2c 11 00 00 00 38 09 00 00 7c 3f 00 00	T7,8|?	success or wait	84	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	16252	2360	76 fd 60 fd fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 32 61 fd fd 7f 00 00 10 00 00 00 00 00 00 00 08 fd 37 2c 11 00 00 00 01 fd 37 2c 11 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 10 1e 2c 11 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 48 fd fd 49 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 78 2f fd fd 49 01 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	v``2a7,7,,HIx/IPP	success or wait	83	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	59170	256	0d 3e fd 06 00 44 fd 3d 3b fd 06 00 4c fd 44 24 70 fd 5c fd fd fd 41 0f fd 4c 5d 00 41 fd 04 fd 48 03 fd fd 02 33 fd 48 fd 5c 24 60 48 fd fd 20 41 5f 41 5e 41 5d 41 5c 5f 5e 5d fd fd fd fd 48 fd 5c 24 10 4c fd 4c 24 20 55 56 57 41 54 41 55 41 56 41 57 48 fd fd 30 48 fd fd 4d fd fd 33 fd 41 fd fd 48 fd fd 48 fd fd 0f fd fd 01 00 00 4d fd fd 0f fd fd 01 00 00 fd fd 0f fd fd 01 00 00 fd 7e 14 50 fd 00 00 0f fd fd 01 00 00 48 fd fd 74 32 39 0a 74 24 fd 02 03 75 1f 33 8b fd fd 37 fd fd 75 15 44 fd 2f 33 8b fd 41 fd fd 02 fd 37 fd fd 41 fd fd 02 73 18 fd 33 02 04 fd fd 01 00 00 fd fd 07 75 fd 41 fd 02 00 00 00 fd fd 03 fd 43 fd 3d fd fd 01 00 0f fd 6a 01 00 00 48 fd fd 0f fd fd 00 00 00 fd 7f 04 02 72 fd 48 39 4f 08 74 49 4c 24 70 fd fd 44 fd 7c 24	>D=;LD$p\AL]AH3H\$`HA_A^A]A_^]H\$LL$UVWATAUAVAWH0HM3AHHM~PHt29t$u37uD/3A7As3uAC=jHrH9OtL$pD|$	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	11208	1232	00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 27 2c 11 00 00 00 fd fd fd fd fd fd fd fd 27 2c 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 68 fd 27 2c 11 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 27 2c 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 68 fd fd 7f 00	3++S++F',',h',',h	success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	1900	48	fd 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 60 1e 2c 11 00 00 00 fd fd 37 2c 11 00 00 00 38 09 00 00 7c 3f 00 00 fd 04 00 00 68 35 00 00	`,7,8|?h5	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	9258	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	25	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	4556	4044	00 00 fd fd fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b fd 26 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 00 00 00 00 14 10 07 fd 49 01 00 00 fd fd 09 fd 49 01 00 00 00 00 07 fd 49 01 00 00 3a 01 00 00 00 00 00 00 fd fd 75 fd fd 7f 00 00 fd fd 75 fd fd 7f 00 00 00 fd 09 fd 49 01 00 00 fd 19 4e fd 0f fd fd 01 14 10 07 fd 49 01 00 00 fd fd 09 fd 49 01 00 00 00 00 07 fd 49 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 3a 01 00 00 00 00 00	<2|h+&BB?#`A pIII:uuINIII:	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	8608	644	01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 01 00 00 00 00 00 50 fd 02 00 00 00 00 65 fd 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 4e fd 00 00 00 00 00 00 0c fd 03 00 00 00 00 00 43 5b 03 00 00 00 00 00 fd 0e 18 00 00 00 00 00 fd fd 07 00 00 00 00 00 40 fd 1f 00 00 00 00 00 12 03 17 00 00 00 00 00 fd fd fd 4a 00 00 00 00 4e fd 7b 1a 00 00 00 00 fd 08 6d 21 00 00 00 00 fd fd fd 01 00 00 00 00 28 fd 00 00 fd 2a 01 00 fd fd 07 00 33 0f 0a 00 fd fd 07 00 4e 23 1a 00 12 03 17 00 f6 65 00 23 fd 01 00 fd fd 1a 00 00 00 00 00 60 fd 4d 00 6e fd 04 00 fd fd 00 00 00 00 00 00 00 00 00 00 11 13 00 00 2e 00 00 00 6d 01 00	ZbPeNC[@JN{m! (*3N#e#`Mn.m	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	59426	5056	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A8C.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0a 00 00 fd 07 00 00 0d 00 00 00 68 0f 00 00 38 12 00 00 05 00 00 00 44 05 00 00 38 3a 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 0c 00 00 02 fd 00 00 15 00 00 00 fd 01 00 00 fd 21 00 00 16 00 00 00 fd 00 00 00 fd 23 00 00	h8D8:`8T!#	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2	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	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	84	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	<WERReportMetadata>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	128	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	<OSVersionInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	180	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	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	270	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	<Build>17134</Build>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	318	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	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	408	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	<Edition>Professional</Edition>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	478	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	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	620	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	<Revision>1</Revision>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	672	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	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	752	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	<Architecture>X64</Architecture>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	824	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	<LCID>1033</LCID>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	864	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	</OSVersionInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	916	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	<ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6792</Pid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 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	<ImageName>rundll32.exe</ImageName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 35 00 33 00 33 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>45331</Uptime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1230	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1316	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	<IptEnabled>0</IptEnabled>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1376	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	<ProcessVmInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1430	96	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 32 00 32 00 30 00 34 00 32 00 30 00 34 00 33 00 36 00 37 00 38 00 37 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	<PeakVirtualSize>2204204367872</PeakVirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1536	80	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 32 00 32 00 30 00 33 00 34 00 30 00 39 00 31 00 30 00 30 00 30 00 38 00 30 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203409100800</VirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1626	78	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 31 00 39 00 37 00 37 00 34 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	<PageFaultCount>197746</PageFaultCount>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1704	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1708	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1714	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 32 00 38 00 37 00 30 00 37 00 30 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>728707072</PeakWorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1814	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1818	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1824	80	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 37 00 39 00 38 00 37 00 32 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7987200</WorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1904	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1908	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	1914	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 30 00 37 00 36 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>107672</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2028	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2032	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2038	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 30 00 37 00 34 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>107472</QuotaPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2136	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2140	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2146	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 34 00 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24152</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2270	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2274	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2280	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 38 00 30 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	<QuotaNonPagedPoolUsage>23800</QuotaNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2388	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2392	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2398	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 37 00 34 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	<PagefileUsage>2174976</PagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2474	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2478	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2484	96	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 30 00 32 00 38 00 31 00 36 00 30 00 30 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>802816000</PeakPagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2580	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2584	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2590	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 37 00 34 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	<PrivateUsage>2174976</PrivateUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2662	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2666	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2670	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	</ProcessVmInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2716	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2720	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2724	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	<ParentProcess>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2754	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2758	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2764	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	<ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2804	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2808	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2816	30	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6740</Pid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2846	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2850	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2858	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 36 00 34 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll64.exe</ImageName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2930	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2934	2	09 00		success or wait	4	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	2942	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3032	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3036	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3044	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 36 00 37 00 37 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>46778</Uptime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3088	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3092	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3100	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3178	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3182	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3190	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	<IptEnabled>0</IptEnabled>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3242	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3246	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3254	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	<ProcessVmInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3298	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3302	2	09 00		success or wait	5	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3312	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 31 00 38 00 32 00 35 00 30 00 39 00 30 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>518250 9056</PeakVirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3402	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3406	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3416	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 34 00 33 00 33 00 38 00 33 00 33 00 39 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	<VirtualSize>4433833984</VirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3490	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3494	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3504	78	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 31 00 39 00 39 00 39 00 38 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	<PageFaultCount>199998</PageFaultCount>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3582	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3586	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3596	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 36 00 30 00 34 00 38 00 33 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>760483840</PeakWorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3696	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3700	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3710	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 30 00 32 00 36 00 30 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>10260480</WorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3792	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3796	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3806	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 32 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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	<QuotaPeakPagedPoolUsage>202160</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3920	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3924	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	3934	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 34 00 34 00 31 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	<QuotaPagedPoolUsage>194416</QuotaPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4032	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4036	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4046	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 31 00 31 00 35 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>11576</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4170	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4174	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4184	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 30 00 38 00 30 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	<QuotaNonPagedPoolUsage>10800</QuotaNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4292	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4296	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4306	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 39 00 30 00 30 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>2990080</PagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4382	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4386	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4396	96	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 30 00 32 00 36 00 36 00 38 00 35 00 34 00 34 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	<PeakPagefileUsage>802668544</PeakPagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4492	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4496	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4506	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 39 00 30 00 30 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>2990080</PrivateUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4578	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4582	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4590	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	</ProcessVmInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4636	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4640	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4646	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	</ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4688	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4692	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4696	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	</ParentProcess>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4728	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4732	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4734	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	</ProcessInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4776	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4780	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4782	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	<ProblemSignatures>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4820	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4824	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4828	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	<EventType>APPCRASH</EventType>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4890	4	0d 00 0a 00		success or wait	8	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4894	2	09 00		success or wait	16	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	4898	104	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 5f 00 4d 00 49 00 70 00 75 00 75 00 53 00 69 00 53 00 5a 00 34 00 2e 00 64 00 6c 00 6c 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	<Parameter0>rundll32.exe_MIpuu SiSZ4.dll</Parameter0>	success or wait	8	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	5554	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	5558	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	5560	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	</ProblemSignatures>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	5600	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	5604	2	09 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	5606	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	<DynamicSignatures>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	5644	4	0d 00 0a 00		success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	5648	2	09 00		success or wait	12	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	5652	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	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6206	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6210	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6212	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	</DynamicSignatures>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6252	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6256	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6258	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	<SystemInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6296	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6300	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6304	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	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6398	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6402	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6406	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 62 00 61 00 68 00 72 00 63 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	<SystemManufacturer>vbahrc, Inc.</SystemManufacturer>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6512	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6516	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6520	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 62 00 61 00 68 00 72 00 63 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	<SystemProductName>vbahrc7,1</SystemProductName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6616	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6620	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6624	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 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 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	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6744	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6748	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6752	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 36 00 31 00 38 00 33 00 30 00 38 00 34 00 36 00 37 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	<OSInstallDate>1618308467</OSInstallDate>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6834	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6838	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6842	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	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6944	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6948	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	6952	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 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	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7020	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7024	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7026	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	</SystemInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7066	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7070	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7072	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	<SecureBootState>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7106	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7110	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7114	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	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7210	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7214	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7216	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	</SecureBootState>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7252	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7256	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7258	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	<Integrator>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7282	4	0d 00 0a 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7286	2	09 00		success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7290	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 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7536	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7540	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7542	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	</Integrator>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7568	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7572	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7574	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 32 00 2d 00 30 00 37 00 2d 00 32 00 32 00 54 00 32 00 31 00 3a 00 31 00 31 00 3a 00 30 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-07-22T21:11:04Z">	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7674	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7678	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7682	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 39 00 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 37 00 39 00 32 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 33 00 34 00 35 00 34 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 34 00 35 00 34 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<Process AsId="398" PID="6792" UptimeMS="34546" TimeSinceCreationMS="34546" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7948	4	0d 00 0a 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7952	2	09 00		success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	7958	198	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 34 00 31 00 31 00 32 00 33 00 38 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="4112384" TimelineUnitShift="12" Timeline="11111111111"/>	success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8362	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8366	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8370	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8390	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8394	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8396	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	</ProcessTimelines>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8434	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8438	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8440	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	<ReportInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8478	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8482	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8486	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 34 00 66 00 64 00 31 00 38 00 66 00 33 00 2d 00 32 00 30 00 62 00 61 00 2d 00 34 00 66 00 66 00 30 00 2d 00 62 00 38 00 35 00 31 00 2d 00 65 00 36 00 64 00 35 00 30 00 63 00 63 00 35 00 37 00 65 00 39 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>d4fd18f3-20ba-4ff0-b851-e6d50cc57e93</Guid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8584	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8588	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8592	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 32 00 2d 00 30 00 37 00 2d 00 32 00 32 00 54 00 32 00 31 00 3a 00 31 00 31 00 3a 00 30 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-07-22T21:11:04Z</CreationTime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8690	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8694	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8696	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	</ReportInformation>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8736	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43B4.tmp.WERInternalMetadata.xml	8740	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	</WERReportMetadata>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4675.tmp.xml	0	4733	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Mlp_773949b15a9dc27bfcd3f791ccbc8dda8da3511_ceeedb37_0e0d5ce9\Report.wer	0	2	fd fd		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Mlp_773949b15a9dc27bfcd3f791ccbc8dda8da3511_ceeedb37_0e0d5ce9\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	150	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Mlp_773949b15a9dc27bfcd3f791ccbc8dda8da3511_ceeedb37_0e0d5ce9\Report.wer	9436	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 32 00 39 00 33 00 34 00 38 00 30 00 30 00 37 00 31 00	MetadataHash=293480071	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{eb3fd99b-4bb8-ff03-929a-4fdd979037b6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC738DE3FE	unknown

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\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 F4 10 00 80 01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 96 00 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 85 17 00 80 01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5C 02 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FFC739007CB	RegSetValueExW

Analysis Process: regsvr32.exe PID: **5852**, Parent PID: **6740**

General

Target ID:	15
Start time:	14:11:03
Start date:	22/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\ZcjkHmdxs\qpwRIIkrlFzB.dll"
Imagebase:	0x7ff6da7e0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **908**, Parent PID: **568**

General

Target ID:	16
Start time:	14:11:04
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6380, Parent PID: 568

General

Target ID:	17
Start time:	14:11:11
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

Analysis Process: svchost.exe PID: 1524, Parent PID: 568

General

Target ID:	18
Start time:	14:11:13
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: 5112, Parent PID: 568

General

Target ID:	19
Start time:	14:11:13
Start date:	22/07/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7b9e90000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **1428**, Parent PID: **568**

General	
Target ID:	20
Start time:	14:11:14
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **7100**, Parent PID: **568**

General	
Target ID:	21
Start time:	14:11:32
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **5604**, Parent PID: **568**

General	
Target ID:	23
Start time:	14:12:03
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MpCmdRun.exe PID: **6256**, Parent PID: **1428**

General	
Target ID:	26
Start time:	14:12:15
Start date:	22/07/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe

Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff7a3c50000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6352**, Parent PID: **6256**

General

Target ID:	27
Start time:	14:12:15
Start date:	22/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **3308**, Parent PID: **568**

General

Target ID:	29
Start time:	14:12:29
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **3052**, Parent PID: **568**

General

Target ID:	32
Start time:	14:12:50
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Disassembly

No disassembly