ID: 671702
Sample Name: MIpuuSiSZ4
Cookbook: default.jbs
Time: 13:55:58
Date: 22/07/2022
Version: 35.0.0 Citrine

Table of Contents

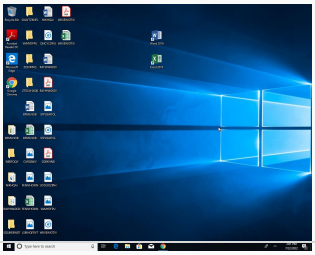
Windows Analysis Report

MIpuuSiSZ4

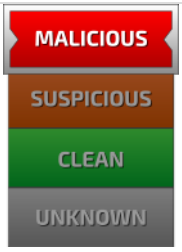
Overview

General Information

Sample Name:	MIpuuSiSZ4 (renamed file extension from none to dll)
Analysis ID:	671702
MD5:	1dd34935a785a4.
SHA1:	c6c966e4ba623f…
SHA256:	8b5a10f9a8f2b25.
Tags:	exe OpenCTIBR Sandboxed
Infos:	



Detection



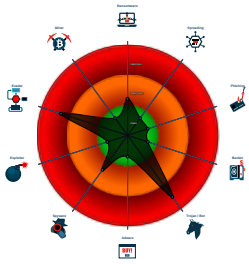
Emotet

Score:	96
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
- 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…
- Contains functionality to query local…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 7160 cmdline: loaddll64.exe "C:\Users\user\Desktop\MIpuuSiSZ4.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6376 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\MIpuuSiSZ4.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6160 cmdline: rundll32.exe "C:\Users\user\Desktop\MIpuuSiSZ4.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 6728 cmdline: C:\Windows\system32\WerFault.exe -u -p 6160 -s 336 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - regsvr32.exe (PID: 5016 cmdline: regsvr32.exe /s C:\Users\user\Desktop\MIpuuSiSZ4.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 5696 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\FmCnbLJkOlaRytmc\QMbXoKRooU.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 3896 cmdline: rundll32.exe C:\Users\user\Desktop\MIpuuSiSZ4.dll,AddStroke MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 4412 cmdline: C:\Windows\system32\WerFault.exe -u -p 3896 -s 328 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - rundll32.exe (PID: 5804 cmdline: rundll32.exe C:\Users\user\Desktop\MIpuuSiSZ4.dll,AddWordsToWordList MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2196 cmdline: rundll32.exe C:\Users\user\Desktop\MIpuuSiSZ4.dll,AdviseInkChange MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 5428 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\YbTPHZsAWIZFUi\eAeQcUPg.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
- svchost.exe (PID: 3316 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6496 cmdline: C:\Windows\system32\WerFault.exe -pss -s 484 -p 6160 -ip 6160 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - WerFault.exe (PID: 6568 cmdline: C:\Windows\system32\WerFault.exe -pss -s 516 -p 3896 -ip 3896 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- svchost.exe (PID: 6584 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4900 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5068 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5928 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7032 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6188 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "192.168.2.7:2",
    "244.26.0.0:1",
    "240.69.242.0:2",
    "184.6.0.0:1",
    "64.6.0.0:1",
    "192.6.0.0:1",
    "244.6.0.0:1",
    "4.7.0.0:1",
    "20.7.0.0:1",
    "76.7.0.0:1",
    "92.7.0.0:1",
    "108.7.0.0:1",
    "112.7.0.0:1",
    "200.6.0.0:1",
    "16.7.0.0:1",
    "96.7.0.0:1",
    "124.7.0.0:1",
    "80.7.0.0:1",
    "128.7.0.0:1",
    "240.6.0.0:1",
    "32.7.0.0:1",
    "36.7.0.0:1",
    "214.112.3.0:5308",
    "241.112.3.0:5164",
    "243.112.3.0:1484"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.457523835.000001A6C0911000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.454942955.0000000001411000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.460329273.0000016A80010000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.500443188.000001A6C0911000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.883306468.0000000001000000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.1a6c08b0000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.rundll32.exe.195c5870000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.0.rundll32.exe.1a6c08b0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.0.rundll32.exe.21313760000.3.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
12.2.regsvr32.exe.1000000.0.raw.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)

Stealing of Sensitive Information

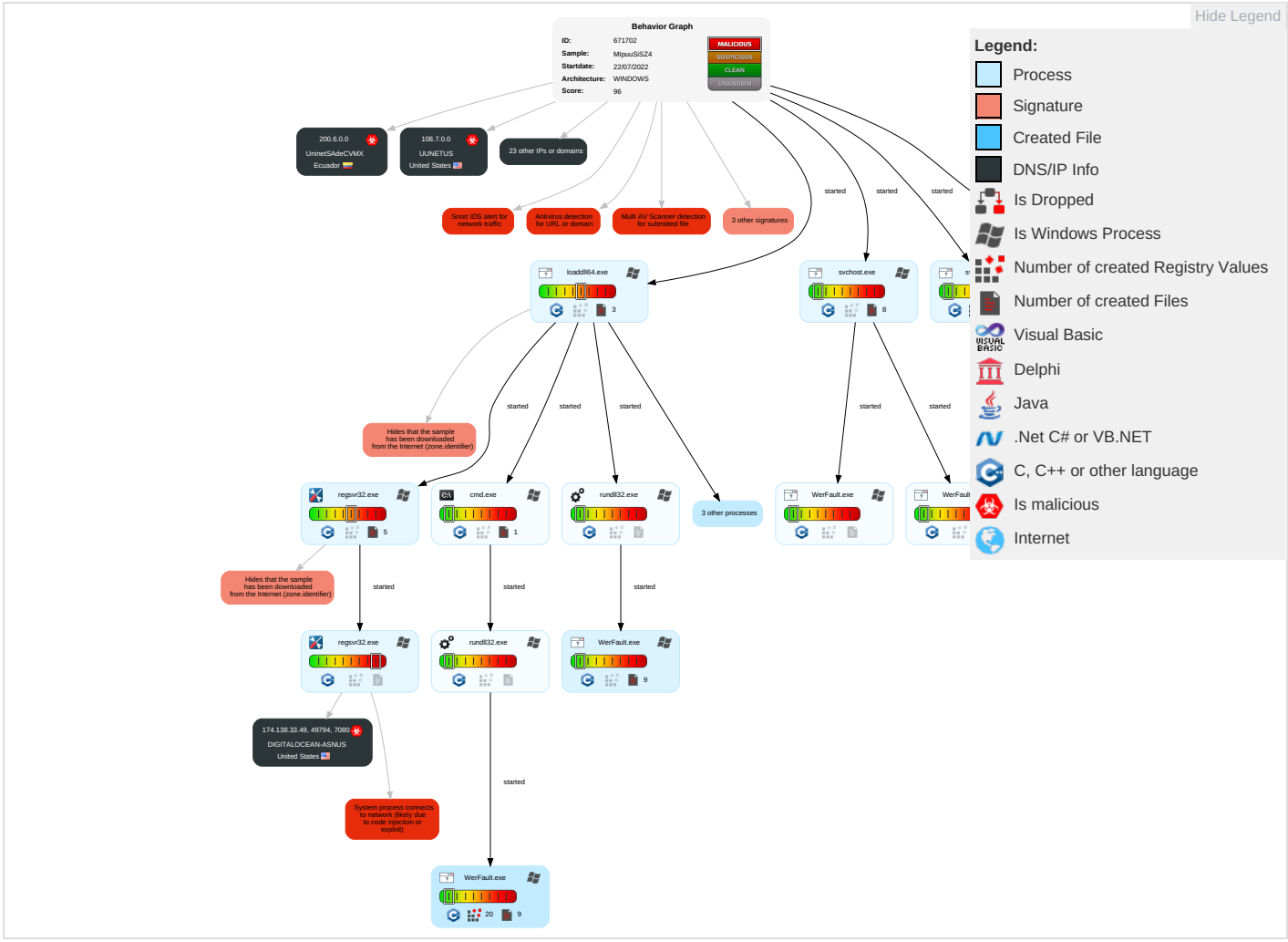
Yara detected Emotet

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
Valid Accounts	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	3 Virtualization/Sandbox Evasion	LSASS Memory	4 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 1 Process Injection	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 Deobfuscate/Decode Files or Information	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 Hidden Files and Directories	LSA Secrets	1 Remote System 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	2 Obfuscated Files or Information	Cached Domain Credentials	2 File and Directory 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	1 Regsvr32	DCSync	4 4 System Information 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 Rundll32	Proc Filesystem	Network Service Scanning	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 DLL Side-Loading	/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 File Deletion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

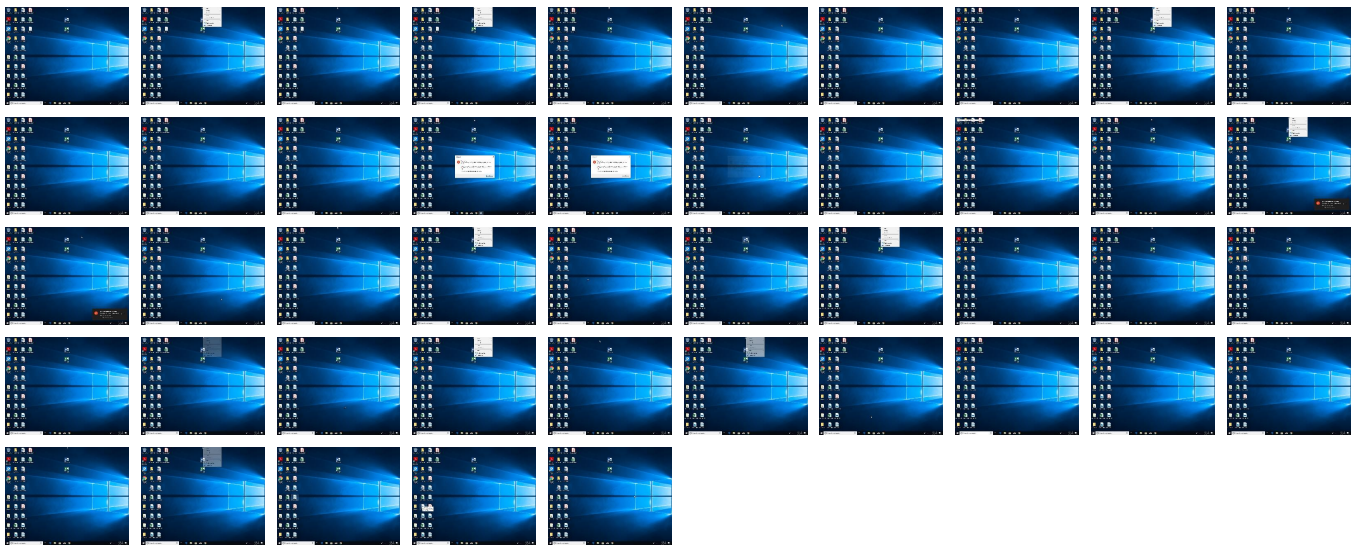
Behavior Graph



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://174.138.33.49/7	100%	Avira URL Cloud	malware	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://174.138.33.49:7080/	0%	URL Reputation	safe	
http://https://174.138.33.49:7080/temy	100%	Avira URL Cloud	malware	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://174.138.33.49:7080/Numv	100%	Avira URL Cloud	malware	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://174.138.33.49/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

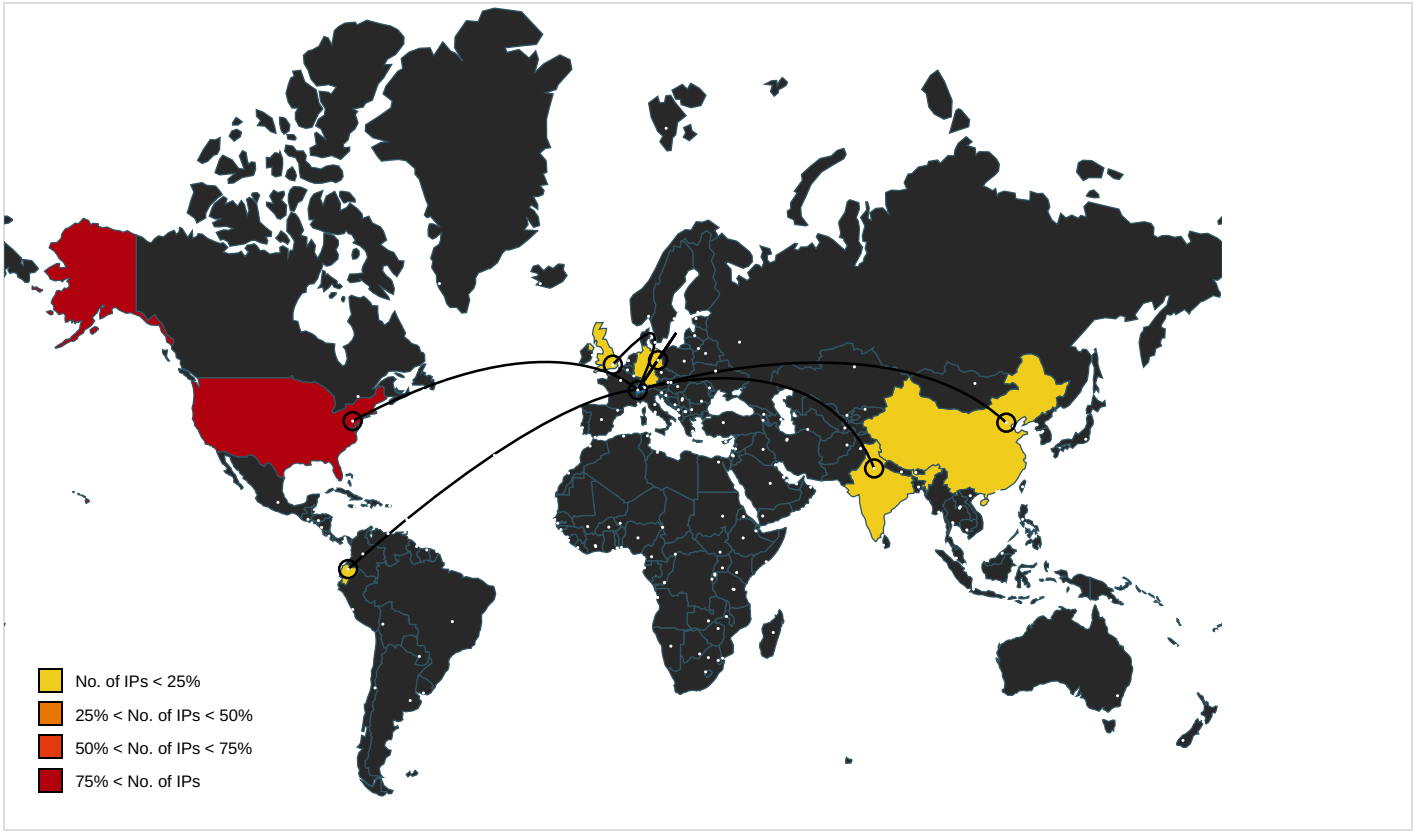
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://174.138.33.49/7	regsvr32.exe, 0000000C.00000003.79240286 9.0000000000EB2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 00C.00000002.882736405.0000000000EB2000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 0000001E.00000003.714545443 .00000147607A0000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 0000001E.00000003.714545443 .00000147607A0000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing	svchost.exe, 00000016.00000002.883340069 .00000227AF8AC000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://174.138.33.49:7080/	regsvr32.exe, 0000000C.00000003.79240286 9.0000000000EB2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 00C.00000002.882736405.0000000000EB2000. 00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.hotspotshield.com/terms/	svchost.exe, 0000001E.00000003.710986823 .0000014760C19000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 E.00000003.710810502.0000014760C02000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.710861874 .0000014760C03000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 E.00000003.710944641.00000147607AD000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.710923120 .000001476079C000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://174.138.33.49:7080/temy	regsvr32.exe, 0000000C.00000003.79240286 9.0000000000EB2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 00C.00000002.882736405.0000000000EB2000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.pango.co/privacy	svchost.exe, 0000001E.00000003.710986823.0000014760C19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.710810502.0000014760C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.710861874.0000014760C03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.710944641.00000147607AD000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.710923120.000001476079C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 0000001E.00000003.714545443.00000147607A0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ver)	svchost.exe, 00000016.00000002.883963436.00000227B5063000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000002.739932682.000001475FCE0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://174.138.33.49:7080/Numv	regsvr32.exe, 0000000C.00000003.792402869.0000000000EB2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000C.00000002.882736405.0000000000EB2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 0000001E.00000003.719101021.00000147607A0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.718967987.00000147607B6000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.719233278.0000014760C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.718937080.00000147607B6000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://help.disneyplus.com.	svchost.exe, 0000001E.00000003.714545443.00000147607A0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.hotspotshield.com/	svchost.exe, 0000001E.00000003.710986823.0000014760C19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.710810502.0000014760C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.710861874.0000014760C03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.710944641.00000147607AD000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000003.710923120.000001476079C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://174.138.33.49/	regsvr32.exe, 0000000C.00000003.792402869.0000000000EB2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000C.00000002.882736405.0000000000EB2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
32.7.0.0	unknown	United States		2686	ATGS-MMD-ASUS	true
174.138.33.49	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
128.7.0.0	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	true
20.7.0.0	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
108.7.0.0	unknown	United States		701	UUNETUS	true
80.7.0.0	unknown	United Kingdom		5089	NTLGB	true
92.7.0.0	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
244.6.0.0	unknown	Reserved		unknown	unknown	true
240.69.242.0	unknown	Reserved		unknown	unknown	true
184.6.0.0	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	true
192.6.0.0	unknown	United States		54735	TTGSIUS	true
112.7.0.0	unknown	China		24444	CMNET-V4SHANDONG-AS-APShandongMobileCommunicationCompany	true
64.6.0.0	unknown	United States		14363	MTCCOMMUS	true
214.112.3.0	unknown	United States		721	DNIC-ASBLK-00721-00726US	true
4.7.0.0	unknown	United States		3356	LEVEL3US	true
76.7.0.0	unknown	United States		22186	CENTURYLINK-LEGACY-EMBARQ-KSGRNRUS	true
96.7.0.0	unknown	United States		262589	INTERNEXABRASILOPERADORADETELECOMUNICACOESSABR	true
240.6.0.0	unknown	Reserved		unknown	unknown	true
243.112.3.0	unknown	Reserved		unknown	unknown	true
200.6.0.0	unknown	Ecuador		8151	UninetSAdeCVMX	true
241.112.3.0	unknown	Reserved		unknown	unknown	true
124.7.0.0	unknown	India		4662	QTCN-ASN1GCNetReachRangeIncTW	true
16.7.0.0	unknown	United States		unknown	unknown	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
36.7.0.0	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	true
244.26.0.0	unknown	Reserved		unknown	unknown	true

Private

IP
192.168.2.1
192.168.2.7
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	671702
Start date and time: 22/07/202213:55:58	2022-07-22 13:55:58 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MIpuuSiSZ4 (renamed file extension from none to 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
Number of analysed new started processes analysed:	32
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:	mal96.troj.evad.winDLL@34/16@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:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 209.197.3.8, 20.189.173.22, 20.189.173.21, 23.35.236.56, 20.223.24.244
- Excluded domains from analysis (whitelisted): onedsblobprdwus17.westus.cloudapp.azure.com, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e12564.dspb.akamaiedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, sls.update.microsoft.com, 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, client.wns.windows.com, fs.microsoft.com, neu-displaycatalogrp.useroor.bigcatalog.commerce.microsoft.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.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

Time	Type	Description
13:58:18	API Interceptor	2x Sleep call for process: WerFault.exe modified
13:58:51	API Interceptor	10x Sleep call for process: svchost.exe modified

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\qmgr.db

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x9bd413be, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2507301596835623
Encrypted:	false
SSDEEP:	384:s+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:zSB2nSB2RSjlK/+mLesOj1J2
MD5:	67BC1180577BCAE7AAAB0395C6668DE1
SHA1:	54063A0EBB7A899A61F7B47C28B184EA080C9FEB
SHA-256:	AADEEC33723E9CB7C975F69645141F65B1CF0545EB6FD12269210108B22083D8
SHA-512:	6AF6B62F9A980A09C1C2CF4A5C7297B156B960DAF9280D7F981356EA56096AA9B765F60FB2FA5D8641B3513A03F4C4736DAF0B9D3F0F368E0F212CC2136240A8
Malicious:	false
Preview:	....e.f.3...w.....&.....w..3:...z..h.(.....3...w.....B.....@..... ....3...w..... ....~...4:...z'..... 4:...z'..... .....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_MIp_773949b15a9dc27bfcd3f791ccbc8dda8da3511_ceeedb37_116bd172\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):	0.7745360116180453
Encrypted:	false
SSDEEP:	192:U5vigJKVHkhyJdJsjIU/u7sVS274ltNw:uviuKFkEJdJsjj/u7sVX4ltNw
MD5:	DC08AF70F1A9F069487A3081FFAE724A
SHA1:	EE7D71A22BEDE02D198F895950703D4BBF73F5F0
SHA-256:	0D736C5C970F822A0FBB017CA75F4894BAF5E23525FAC93D52720D575D247A4C
SHA-512:	3475021FFDAAD7B6D5AB9ACEE4E5B84B5091AAB192565EB29BAD694D46083E132F31B3B2D157E4346942580D4224FC3FE4743B998935740FFD724E7CDACE20F7
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.=.1.3.3.0.2.9.9.7.0.8.6.8.5.0.3.1.2.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.0.2.9.9.7.0.9.7.4.4.3.9.5.7.2.....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.=.8.c.a.2.3.b.0.8.-.5.7.9.2.-.4.d.9.b.-.8.d.e.9.-.f.0.c.9.f.e.9.2.8.a.9.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.c.f.e.3.b.9.1.-.d.9.1.4.-.4.7.d.9.-.a.8.c.7.-.7.7.4.6.f.5.f.d.b.9.d.9.....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.=.0.0.0.0.0.f.3.8.-.0.0.0.1.-.0.0.1.8.-.1.5.a.5.-.5.6.9.e.0.d.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_1a1fcd1c\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):	0.7735005926866978
Encrypted:	false
SSDEEP:	96:aRFnliyQijJPny2jT55I73f2pXIQcQqc620ycEBcw3pXaXz+HbHgSQgJPbwGIDVU:KfixijJKSHkhyLtjIU/u7sVS274ltN
MD5:	A86B7FADCDE51D62CE966354FB5F6D3E
SHA1:	3CDC004C4F0E8C87DEDE02051BD08E5733D5A620
SHA-256:	62D635E063040B7F760E0424452183FB2DBA728192E3559036CECF5DB0A4B868
SHA-512:	686DCADB722410A0A0AC4884411C4742CADB7CE3A81E9B5C38F2C63480FEBCE141912E5E577C73DF0B6D13DF7E6E346CEF1E8F44FD7708E28AE28F3C19EEA75F
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.=.1.3.3.0.2.9.9.7.0.8.3.8.3.0.0.4.2.3.....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.=.1.3.3.0.2.9.9.7.0.9.6.3.7.6.7.9.4.8.....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.=.8.7.4.5.6.d.6.a.-.4.a.0.3.-.4.1.1.2.-.b.6.0.2.-.7.6.1.0.4.9.f.7.9.0.2.9.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.0.b.7.e.3.e.8.-.e.b.a.b.-.4.1.8.e.-.8.7.f.f.-.b.e.7.a.0.0.9.2.5.9.8.1.....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.=.0.0.0.0.1.8.1.0.-.0.0.0.1.-.0.0.1.8.-.8.8.1.e.-.1.0.9.e.0.d.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\WER940B.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Jul 22 20:58:11 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	63490
Entropy (8bit):	2.3463206366673157
Encrypted:	false
SSDEEP:	384:DIyacvV4z7BXVjaKChYAFwvpMlwdbA5AQ:fact4x1COGqbV
MD5:	6DA5CE983BAF9352E00714A8BB39727E
SHA1:	40AC6315F73498356FFD4546AB837B1EDB8E4436
SHA-256:	E1FDAEE089B49ED19476BC82FEADFAC287A65FD3F7FE361C64BEA1CA72FF9F49
SHA-512:	8B22B9B1C1F8DE25E6B994F2143D6D08F4DC8C2285CCADD2968A612209FC7C69CD9849FBD9D6FA9A7BDD322E16B9203585199853F6824CA1C5D4A5895726511
Malicious:	false
Preview:	MDMP..... .....c..b.....h...8.....D...8:.....`.....8.....T.....Z.....I.....#.....U.....B.....$$.....Lw.....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\WER9FD2.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Jul 22 20:58:12 2022, 0x1205a4 type
Category:	dropped

Size (bytes):	64526
Entropy (8bit):	2.3013812479784215
Encrypted:	false
SSDEEP:	192:0VlvLya1EV4zKQBXVjLSp/JwKOC5CZ5HtitAzdQG0wdS3oCwcPxAX/WjwGvnMrsQ:gyaSV4z7BXVjaeCsTNglwdI4CwG0oH
MD5:	EA3866323B1704449AD420AFF2568E70
SHA1:	A8D86FB576FDACCE09830A84D42D6BEF00BEE8A6
SHA-256:	A076EBFBE6DE8900FA059902F628D87B656F7CA5652162CEFB772D406A486FB2
SHA-512:	A656792FD06E4857B793F3473899619DEEA32D8E33F2706EE12D7D7661618DBDB13558F1908D79D48E38834149EFD3B7608D4CFF570BF3DA0D7CC2AE5467774
Malicious:	false
Preview:	MDMP..... .....d..b.....h...8.....T...8:.....`.....8.....T.....X.....!.....#.....U.....B.....$$... ...Lw.....$\a...T.....8...)..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\WERB4E2.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):	8756
Entropy (8bit):	3.699929917648694
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiUdXVS236Yn8Orgmf1RS/9XCprk89bLHexfCl5m:RrlsNiuXVSG6Y8Orgmf1RSVmLHgfCy
MD5:	5707F8FB038E671C7B62CB5035AAAB02
SHA1:	74C594EF9DA77B7F4D233D5F7F6C1961A4D7A113
SHA-256:	7E3AA329FF2FDBF29AFBBAC46A16C4268399B33CF15B4D0105AC15CCD4ADB59E
SHA-512:	882B94720EE909570C32FAC048E9AEF2EC5D5F6374061B7CEAF8B57740ADB0611D89424E18CDEAE72D2ED828B82F6E00EE20085174520DDD56E7BA9EA396D235
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.>.6.1.6.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB764.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):	4.4845182631342055
Encrypted:	false
SSDEEP:	48:cvIwSD8zsqJgtBI9oeWgc8sqYjX8fm8M4JC/WC/J8FHPyq85m/E8pkZESC5S0d:uITf4qfgrsqYlJ8baP9FmVv0d
MD5:	1ADF8A480754A46C16ABB3071BBDE030
SHA1:	4296C5D7A325C8AA4A1EE0E4D31C842A9B7A7F51
SHA-256:	FF255A547C95F1D3E34B22ABD7F4E29D2F61796538E64A29E0C19F082BAAEC36
SHA-512:	1EA031B7241D3D88449510EB32C833A9EE93CFFF6B4F91D14A38D9977D2243F78126688445C124252333F9F172BB02A1D857D5F367641E92C98E5C9A8D208D67
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="1614608" />.. <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\WERB89A.tmp.csv

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	53366
Entropy (8bit):	3.039602557285005
Encrypted:	false

SSDEEP:	1536:7pHolfWew9msUxoufVGpupKCxx8a4JIR1efcW6qbwYsbTRVK:7pHolfWew9msUxoufVGpupKax8a4JIRM
MD5:	AD9B2D87A8B0A0650C811F0196D3FC69
SHA1:	E589D91FD2A256451BDD824C34DC087AA4C18F99
SHA-256:	8D499200DC2DC20F84F58BC3CB5E051FA9854AFA7A889D84EED09EE5F81E49A5
SHA-512:	FFFD113868323A53C6453B1A351B18CA23079C23C0E839E96EB776983F70B86184A21413DE003E518D8133820935F665E6A9F9BD64A3B719D15055D6E7CE766B
Malicious:	false
Preview:	l.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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):	3.7024676918374104
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi5M4SC6YZiD/dgmf15S/3J0XCprpx89b90qf+7fm:RrlsNiC4SC6Y8D/dgmf15SvJ0P9pf+K
MD5:	351B391DF4BC5442150F6F2B00D5BD60
SHA1:	79BD5E9F2C1D8B703125E7E0DBC2F0451C6E048E
SHA-256:	A3451CB058B5E7CD354B15B5414F4845CD0C6E54A6A823D4BE11F550011DEB0D
SHA-512:	8074FDBA7BBBDFDB2945D905D8E20222A7DEFB83EB731847D8F152892F92E505CD144413115FA7208F08924309D7AEBB268BFFB4665FD24B1B75CB8C7903DC74
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.8.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE49.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):	4.488917511624953
Encrypted:	false
SSDEEP:	48:cvIwSD8zsqJgtBI9oeWgc8sqYj1a8fm8M4JC/WC/JsFP+yq85m/EkZESC5SRd:uITf4qfgrsqYpvJ8b6+9hVvRd
MD5:	03A8266176247D4230025BA8D9AF1772
SHA1:	FED690D9A1A7086A597B418949F8C37323751285
SHA-256:	AA9C108A14F8B04E30FD522AF6327172D809E5DD94B8668DDA229D1CF9CD988C
SHA-512:	92A1E68401BE0F368347E41EBD3BAF3241567D6C387E9A465AB8D0E66AA13E3360ABE225679C7BA24203C83E48E2284351A28C1071DE13631B80FE2DF8E8BB05
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="1614608" />.. <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\WERC0F8.tmp.csv

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	53030
Entropy (8bit):	3.0405121690366794
Encrypted:	false
SSDEEP:	1536:qmHjfXV+vnUwuufdGpupKCxqgafJIRbefeZUNjYs0rG:qmHjfXV+vnUwuufdGpupKaqgafJIRbe5
MD5:	7D1A88D60AF131C65C41EAF82B0BDEDA

SHA1:	606F6D475DB41C98C1C3A50E9ADFDBD3933E5F57
SHA-256:	837BCFBD3BC1953219F1DB90CBE1B34E991CE28DA0AD3F9D3AE530A916061087
SHA-512:	A439134254BF5E700398ED342298DB0DBBA141D8B167701E01A073166C2AC6CBC70D3372E91BA33C0920BF7C6F3181D3946D3E0B330362782E0560E2D41A08E
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC28F.tmp.txt

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.7042695129115457
Encrypted:	false
SSDEEP:	96:kiZYWR4EGQY0iYGQPiHSUYEZBOt8iOO78dwaWuzraoLRtKlcNIcNy:hZDNELvWuXaoLRtKGScNy
MD5:	D113A605C42A9F5B80205B269AFE4CD8
SHA1:	CF90AA4AB1E3B96324E23C137534C2724086C13A
SHA-256:	E75D7414ADD5AEFF36D29530716015AF2E6141BB95B1A7C35606363169D1143A
SHA-512:	FCBD8EB398D82EB7B866C6EC6B4305C8448AB5AFE4C36DC04F091301423177BBAD8ACA98D9A62D56574EF3DE0D4B76456E3C489B69B78DC84E8496FED1897CB
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.2.6.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6A7.tmp.txt

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.7045158693525706
Encrypted:	false
SSDEEP:	96:kiZYWGMk+kONYxYSQOpHSUYEZpst8i5O78qwTSG8PtDaGL1DKlcNIbNy:hZDGtSGTQSZtDaGL1DKGSbNy
MD5:	DDA604DCF734EE681590803CEC9FAFE3
SHA1:	862AA166DA42679D7DCA16A4273F829C04FA219E
SHA-256:	6444E6B751946D2B298A87E8EA6589E582E2DD588F5D4790B59A8952EA6F862D
SHA-512:	FA7D844BB510EFE0F1A4BE13AAFA94E94216AD0D6B7290B3AD505E7E3D17435531855D911A135B38C73E99CECA0DD0D0C8EB068FBB21CE2B83F128D66F7A5E2B
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.2.6.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

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:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E94155B

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.....ul.....}.....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):	3.1297566246827087
Encrypted:	false
SSDEEP:	6:kKme+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:+eNkPlE99SNxAhUeE1
MD5:	A42B93B0EC145424B2143A7E54D44391
SHA1:	46B8C15CCF1EEB1A3E06B2AD72434B33E8466FB7
SHA-256:	9B6D154A211EA55DA2EF86DCEDA82C22BD0868650C70EE05239917587950244E
SHA-512:	80B432F4390423D2D7CF28FDFC1D4DFAAEFF939B3576F745775F0FD674F1517C4C10E1BB7B3193506F8A4795DD0DDF5C0C9438DE91A42415F1E40CF5802D81E
Malicious:	false
Preview:	p..... .....k.'.....(..... .....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"}

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 00007F0048B8B8E7h
call 00007F0048B8BF9Ch
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 00007F0048B8B750h
int3
int3
int3

Instruction
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 00007F0048B8D6B0h
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
inc eax
push ebx
dec eax

Instruction
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

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

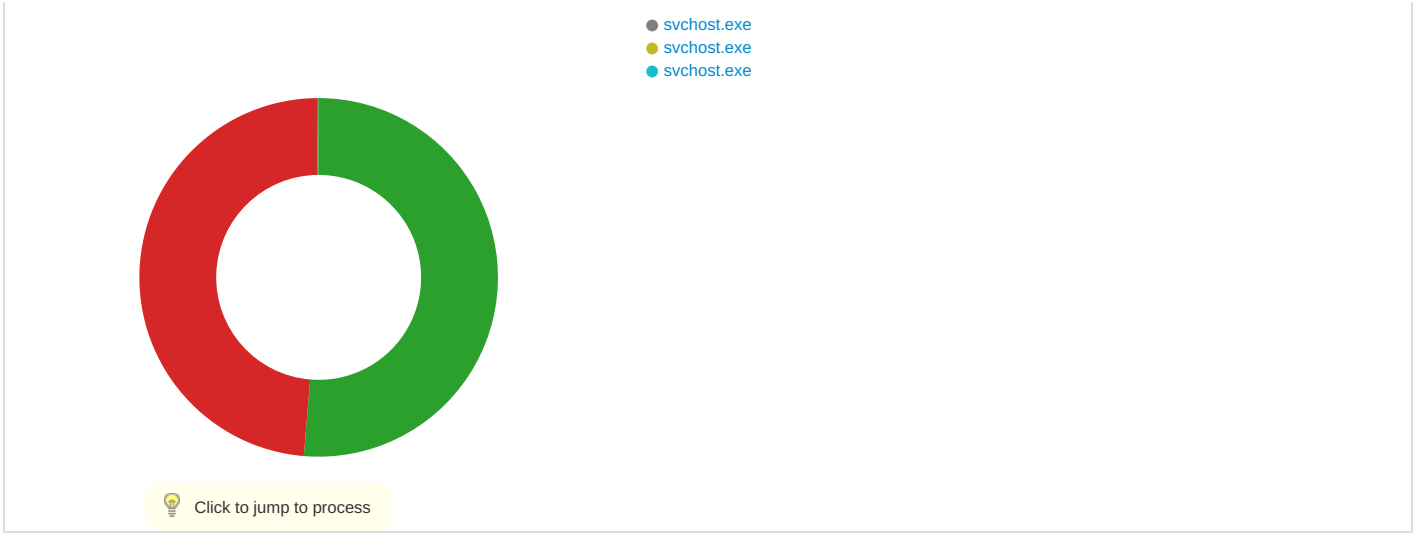
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 22, 2022 13:58:44.263206959 CEST	49794	7080	192.168.2.7	174.138.33.49
Jul 22, 2022 13:58:44.370028973 CEST	7080	49794	174.138.33.49	192.168.2.7
Jul 22, 2022 13:58:44.370176077 CEST	49794	7080	192.168.2.7	174.138.33.49
Jul 22, 2022 13:58:44.402960062 CEST	49794	7080	192.168.2.7	174.138.33.49
Jul 22, 2022 13:58:44.509370089 CEST	7080	49794	174.138.33.49	192.168.2.7
Jul 22, 2022 13:58:44.540781021 CEST	7080	49794	174.138.33.49	192.168.2.7
Jul 22, 2022 13:58:44.540803909 CEST	7080	49794	174.138.33.49	192.168.2.7
Jul 22, 2022 13:58:44.540869951 CEST	49794	7080	192.168.2.7	174.138.33.49
Jul 22, 2022 13:58:44.540894985 CEST	49794	7080	192.168.2.7	174.138.33.49
Jul 22, 2022 13:58:51.413127899 CEST	49794	7080	192.168.2.7	174.138.33.49
Jul 22, 2022 13:58:51.526726961 CEST	7080	49794	174.138.33.49	192.168.2.7
Jul 22, 2022 13:58:51.526912928 CEST	49794	7080	192.168.2.7	174.138.33.49
Jul 22, 2022 13:58:51.534461975 CEST	49794	7080	192.168.2.7	174.138.33.49
Jul 22, 2022 13:58:51.682136059 CEST	7080	49794	174.138.33.49	192.168.2.7
Jul 22, 2022 13:58:52.064332008 CEST	7080	49794	174.138.33.49	192.168.2.7
Jul 22, 2022 13:58:52.064538002 CEST	49794	7080	192.168.2.7	174.138.33.49
Jul 22, 2022 13:58:55.067655087 CEST	7080	49794	174.138.33.49	192.168.2.7
Jul 22, 2022 13:58:55.067689896 CEST	7080	49794	174.138.33.49	192.168.2.7
Jul 22, 2022 13:58:55.067923069 CEST	49794	7080	192.168.2.7	174.138.33.49
Jul 22, 2022 14:00:36.722028017 CEST	49794	7080	192.168.2.7	174.138.33.49
Jul 22, 2022 14:00:36.722055912 CEST	49794	7080	192.168.2.7	174.138.33.49

Statistics

Behavior

- loaddll64.exe
- cmd.exe
- regsvr32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- svchost.exe
- WerFault.exe
- regsvr32.exe
- WerFault.exe
- svchost.exe
- WerFault.exe
- WerFault.exe
- regsvr32.exe
- svchost.exe
- svchost.exe



System Behavior

Analysis Process: loaddll64.exe PID: 7160, Parent PID: 5056

General

Target ID:	0
Start time:	13:57:12
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:	0x7ff620870000
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: 00000000.00000002.488615007.000001942A671000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.488528971.000001942A5D0000.00000040.00001000.00020000.00000000.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: 6376, Parent PID: 7160

General

Target ID:	1
Start time:	13:57:12
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:	0x7ff6a6590000
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: **5016**, Parent PID: **7160**

General

Target ID:	2
Start time:	13:57:13
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:	0x7ff655380000
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: 00000002.00000002.454942955.0000000001411000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.454887422.00000000013B0000.00000040.00001000.00020000.00000000.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\FmCnbLJkOlaRytmc\QMbXoKRooU.dll:Zone.Identifier	success or wait	1	142ED93	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: **6160**, Parent PID: **6376**

General

Target ID:	3
Start time:	13:57:13
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:	0x7ff66c6b0000
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: 00000003.00000000.457523835.000001A6C0911000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.500443188.000001A6C0911000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.499993940.000001A6C08B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.457466014.000001A6C08B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.448855621.000001A6C0911000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.448792384.000001A6C08B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **3896**, Parent PID: **7160**

General

Target ID:	4
Start time:	13:57:13
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:	0x7ff66c6b0000
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: 00000004.00000002.503233757.0000021313901000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.458204040.0000021313901000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.457983091.0000021313760000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.454361313.0000021313901000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.454167344.0000021313760000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.503043476.0000021313760000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **5804**, Parent PID: **7160**

General

Target ID:	5
Start time:	13:57:17
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:	0x7ff66c6b0000
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: 00000005.00000002.460329273.0000016A80010000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.460399040.0000016A80071000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **2196**, Parent PID: **7160**

General	
Target ID:	6
Start time:	13:57:21
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:	0x7ff66c6b0000
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: 00000006.00000002.468293754.00000195C58D1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.468234789.00000195C5870000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: **3316**, Parent PID: **604**

General	
Target ID:	10
Start time:	13:57:51
Start date:	22/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff7e8070000
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	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **6496**, Parent PID: **3316**

General	
Target ID:	11
Start time:	13:57:52
Start date:	22/07/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -pss -s 484 -p 6160 -ip 6160
Imagebase:	0x7ff7fe6b0000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0

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

Analysis Process: regsvr32.exe PID: **5696**, Parent PID: **5016**

General

Target ID:	12
Start time:	13:57:54
Start date:	22/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\FmCnbLJkOlaRytmc\QMbXoKRooU.dll"
Imagebase:	0x7ff655380000
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.00000002.883306468.0000000001000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.883481925.0000000002861000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_3, Description: , Source: 0000000C.00000002.882519844.0000000000E78000.00000004.00000020.00020000.00000000.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: **6568**, Parent PID: **3316**

General

Target ID:	13
Start time:	13:57:55
Start date:	22/07/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -pss -s 516 -p 3896 -ip 3896
Imagebase:	0x7ff7fe6b0000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **6584**, Parent PID: **604**

General

Target ID:	14
Start time:	13:57:55
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:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: **6728**, Parent PID: **6160**

General

Target ID:	15
Start time:	13:58:01
Start date:	22/07/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6160 -s 336
Imagebase:	0x7ff7fe6b0000
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	7FF8C976527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB764.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB764.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_MIp_aa8bb9fdf8d32e2840ca8df43968d536d04b9a9_ceeedb37_1a1fcd1c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_MIp_aa8bb9fdf8d32e2840ca8df43968d536d04b9a9_ceeedb37_1a1fcd1c\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8C975E9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB764.tmp	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp.dmp	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB764.tmp.xml	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB89A.tmp.csv	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC28F.tmp.txt	success or wait	1	7FF8C975E9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 63 0f fd 62 fd 05 12 00 00 00 00 00	MDMP cb	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp.dmp	9252	6	00 00 00 00 00 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.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 1f fd 02 00 00 54 05 00 00 fd 03 00 00 10 18 00 00 29 0f 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 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$$LwT)b0Pacific Standard TimePacific Daylight Time	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp.dmp	9976	1232	00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 6b 6c fd 7f 00 00 00 00 00 00 00 00 00 00 00 12 4a fd fd 01 00 00 fd 57 2e 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 fd fd fd 75 38 00 00 00 fd 03 04 00 00 00 00 00 00 00 6b 6c fd 7f 00 00 00 00 6b 6c fd 7f 00 00 fd fd fd 75 38 00 00 00 fd fd fd 75 38 00 00 00 fd 03 04 00 00 00 00 00 fd 03 04 00 00 00 00 00 fd 57 fd 01 00 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 00 fd 57 fd 01 00 00 fd 10 00 fd 01 00 00	klJW._3++S++u8klklu8u8 W0W	success or wait	1	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp.dmp	1632	168	34 05 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 03 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 fd 26 00 00	4&	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp.dmp	14904	20	54 00 00 00 58 fd fd 75 38 00 00 00 fd 07 00 00 7c 3f 00 00	TXu8|?	success or wait	84	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp.dmp	16252	1960	76 fd fd fd fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 32 fd fd fd 7f 00 00 10 00 00 00 00 00 00 00 fd fd fd 75 38 00 00 00 fd fd fd 75 38 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 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 fd fd 75 38 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 40 48 fd 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 fd 30 fd 01 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 00 00 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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`2u8u8u8@H0XX	success or wait	83	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp.dmp	57890	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;rL HI.4M3IM5Hu)L;s)"	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp.dmp	11208	1232	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 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 75 38 00 00 00 fd fd fd fd fd fd fd fd fd fd 75 38 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 28 fd fd 75 38 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 fd 75 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 7f 00	3++S++Fu8u8(u8u8	success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp.dmp	1900	48	54 11 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 fd 75 38 00 00 00 58 fd fd 75 38 00 00 00 fd 07 00 00 7c 3f 00 00 fd 04 00 00 68 35 00 00	T Pu8Xu8|?h5	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.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 fd fd fd 01 00 00 fd d3 fd fd 01 00 00 00 00 fd fd fd 01 00 00 3a 01 00 00 00 00 00 00 fd fd fd fd fd 7f 00 00 fd fd fd fd fd 7f 00 00 00 fd fd fd 01 00 00 4a 0f fd fd 0d fd fd 01 14 10 fd fd fd 01 00 00 fd d3 fd fd 01 00 00 00 00 fd fd fd 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 3a 01 00 00 00 00 00	<2|h+&BB?#`A p:J:	success or wait	1	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.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 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 01 00 00 00 00 00 fd fd 02 00 00 00 00 fd 14 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 51 fd 00 00 00 00 00 00 06 fd 03 00 00 00 00 00 fd 66 03 00 00 00 00 00 43 fd 17 00 00 00 00 00 fd 26 08 00 00 00 00 00 40 fd 1f 00 00 00 00 00 56 3a 17 00 00 00 00 00 fd fd 75 00 00 00 00 fd fd fd 1e 00 00 00 00 fd 6f 5b 21 00 00 00 00 fd 12 fd 01 00 00 00 00 79 0e 01 00 fd 1a 01 00 fd 5c 07 00 fd 1c 0a 00 fd 26 08 00 fd 1f 1a 00 56 3a 17 00 fd 71 00 fd fd 01 00 fd 5f 1d 00 00 00 00 00 fd fd 57 00 01 fd 04 00 5a fd 00 00 00 00 00 00 00 00 00 00 09 12 00 00 39 00 00 00 70 02 00	ZbQfC&@V:uo[!y\&V:q_WZ9p	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.tmp.dmp	58146	5344	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 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	EventFileFile(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTim	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER940B.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 0d 00 00 5a 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:`8TZ!#	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6160</Pid>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 39 00 31 00 33 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>59131</Uptime>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 30 00 31 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2204204380160 </PeakVirtualSize>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 38 00 33 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>197837</PageFaultCount>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1704	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1708	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 36 00 38 00 33 00 37 00 34 00 31 00 31 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>683741184</PeakWorkingSetSize>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1814	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1818	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 35 00 34 00 34 00 33 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7954432</WorkingSetSize>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1904	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	1908	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 37 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>107784</QuotaPeakPagedPoolUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2028	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2032	2	09 00		success or wait	3	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>107584</QuotaPagedPoolUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2136	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2140	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2270	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2274	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2388	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2392	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 38 00 33 00 31 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>2183168</PagefileUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2474	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2478	2	09 00		success or wait	3	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 31 00 39 00 30 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>802811904</PeakPagefileUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2580	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2584	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 38 00 33 00 31 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>2183168</PrivateUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2662	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2666	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2716	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2720	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2754	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2758	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2804	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2808	2	09 00		success or wait	4	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2816	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6376</Pid>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2846	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2850	2	09 00		success or wait	4	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3032	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 39 00 36 00 35 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>59659</Uptime>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3166	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3170	2	09 00		success or wait	4	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3230	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3234	2	09 00		success or wait	4	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3286	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3290	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3396	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3400	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3490	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3494	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>790</PageFaultCount>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3576	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3580	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 33 00 36 00 38 00 33 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>2936832</PeakWorkingSetSize>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3686	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3690	2	09 00		success or wait	5	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 34 00 35 00 34 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>2924544</WorkingSetSize>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3780	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3784	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3906	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3910	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	3920	96	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 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 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	<QuotaPagedPoolUsage>27664</QuotaPagedPoolUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4016	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4020	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4152	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4156	2	09 00		success or wait	5	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4272	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4276	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 38 00 34 00 38 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>2084864</PagefileUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 33 00 37 00 35 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3137536</PeakPagefileUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4468	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4472	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 38 00 34 00 38 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>2084864</PrivateUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	8	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	16	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	5530	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	5534	2	09 00		success or wait	1	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	5576	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	5580	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	5620	4	0d 00 0a 00		success or wait	6	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	5624	2	09 00		success or wait	12	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6182	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6186	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6228	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6232	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6272	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6276	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6374	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6378	2	09 00		success or wait	2	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 6e 00 62 00 63 00 6e 00 6c 00 68 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>nbcnlh, Inc.</SystemManufacturer>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6488	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6492	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 6e 00 62 00 63 00 6e 00 6c 00 68 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>nbcnlh7,1</SystemProductName>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6592	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6596	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6720	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6724	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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 36 00 34 00 38 00 36 00 39 00 32 00 30 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>1616486920</OSInstallDate>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6810	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6814	2	09 00		success or wait	2	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6920	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6924	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7042	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7046	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7082	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7086	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7186	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7190	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7228	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7232	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7258	4	0d 00 0a 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7262	2	09 00		success or wait	6	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7514	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7518	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7520	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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7546	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7550	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7552	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 30 00 3a 00 35 00 38 00 3a 00 31 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-07-22T20:58:12Z">	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7652	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7656	2	09 00		success or wait	2	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7660	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 34 00 30 00 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 36 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 37 00 39 00 36 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 37 00 39 00 36 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="403" PID="6160" UptimeMS="37968" TimeSinceCreationMS="37968" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7926	4	0d 00 0a 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7930	2	09 00		success or wait	6	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	7936	202	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 35 00 35 00 33 00 33 00 36 00 39 00 36 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 30 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="5533696" TimelineUnitShift="12" Timeline="10111 11111111"/>	success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8338	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8342	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8346	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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8366	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8370	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8372	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	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8410	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8414	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8416	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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8454	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8458	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8462	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 37 00 34 00 35 00 36 00 64 00 36 00 61 00 2d 00 34 00 61 00 30 00 33 00 2d 00 34 00 31 00 31 00 32 00 2d 00 62 00 36 00 30 00 32 00 2d 00 37 00 36 00 31 00 30 00 34 00 39 00 66 00 37 00 39 00 30 00 32 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>87456d6a-4a03-4112-b602-761049f79029</Guid>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8560	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8564	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8568	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 30 00 3a 00 35 00 38 00 3a 00 31 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-07-22T20:58:12Z</CreationTime>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8666	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8670	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8672	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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8712	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB4E2.tmp.WERInternalMetadata.xml	8716	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	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB764.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Mlp_aa8bb9fdf8d32e2840ca8df43968d536d04b9a9_ceeedb37_1a1fcd1c\Report.wer	0	2	fd fd		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Mlp_aa8bb9fdf8d32e2840ca8df43968d536d04b9a9_ceeedb37_1a1fcd1c\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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Mlp_aa8bb9fdf8d32e2840ca8df43968d536d04b9a9_ceeedb37_1a1fcd1c\Report.wer	9444	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 35 00 32 00 34 00 39 00 38 00 37 00 35 00 39 00 37 00	MetadataHash=1524987597	success or wait	1	7FF8C975E9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: WerFault.exe PID: **4412**, Parent PID: **3896**

General

Target ID:	16
Start time:	13:58:02
Start date:	22/07/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 3896 -s 328
Imagebase:	0x7ff7fe6b0000
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	7FF8C976527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE49.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE49.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_MIp_773949b15a9dc27bfcd3f791ccbc8dda8da3511_ceeedb37_116bd172	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_MIp_773949b15a9dc27bfcd3f791ccbc8dda8da3511_ceeedb37_116bd172\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8C975E9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE49.tmp	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp.dmp	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE49.tmp.xml	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0F8.tmp.csv	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6A7.tmp.txt	success or wait	1	7FF8C975E9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 64 0f fd 62 fd 05 12 00 00 00 00 00	MDMP db	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp.dmp	9252	6	00 00 00 00 00 00		success or wait	1	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.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 24 5c 61 01 00 00 54 05 00 00 fd 03 00 00 38 0f 00 00 29 0f 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 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$$Lw$\aT8)b0Pacific Standard TimePacific Daylight Time	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp.dmp	9976	1232	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 57 fd 13 00 00 00 00 fd 02 00 00 fd 7f 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 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 00 00 00 44 17 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 6b 6c fd 7f 00 00 fd 57 fd 13 00 00 00 00 fd fd fd 34 65 00 00 00 fd fd fd 34 65 00 00 00 48 00 08 00 00 00 00 00 00 00 6b 6c fd 7f 00 00 fd 57 fd 13 13 02 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 30 57 fd 13 13 02 00 00 0a 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 08 22 fd 13 13 02 00 00 fd 17 00 fd 01 00 00	W_3++S++DklW4e4eHkl W00W"	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp.dmp	1632	168	fd 15 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 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp.dmp	14904	20	55 00 00 00 00 12 13 13 02 00 00 2e 00 00 00 fd 3f 00 00	U.?	success or wait	85	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp.dmp	16268	46	01 0f 06 00 0f 34 0c 00 0f 72 08 70 07 60 06 50 01 09 02 00 09 32 02 50 01 17 09 00 17 01 24 00 0b fd 09 fd 07 fd 05 70 04 60 03 30 02 50	4rp`P2P$p`0P	success or wait	84	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp.dmp	59034	256	0d 3e fd 06 00 44 fd 3d 3b fd 06 00 4c fd 44 24 70 fd 5c fd fd fd 41 0f fd 4c 5d 00 41 fd 04 fd 48 03 fd fd 02 33 fd 48 fd 5c 24 60 48 fd fd 20 41 5f 41 5e 41 5d 41 5c 5f 5e 5d fd fd fd fd 48 fd 5c 24 10 4c fd 4c 24 20 55 56 57 41 54 41 55 41 56 41 57 48 fd fd 30 48 fd fd 4d fd fd 33 fd 41 fd fd 48 fd fd 48 fd fd 0f fd fd 01 00 00 4d fd fd 0f fd fd 01 00 00 fd fd 0f fd fd 01 00 00 fd 7e 14 50 fd 00 00 0f fd fd 01 00 00 48 fd fd 74 32 39 0a 74 24 fd 02 03 75 1f 33 8b fd fd 37 fd fd 75 15 44 fd 2f 33 8b fd 41 fd fd 02 fd 37 fd fd 41 fd fd 02 73 18 fd 33 02 04 fd fd 01 00 00 fd fd 07 75 fd 41 fd 02 00 00 00 fd fd 03 fd 43 fd 3d fd fd 01 00 0f fd 6a 01 00 00 48 fd fd 0f fd fd 00 00 00 fd 7f 04 02 72 fd 48 39 4f 08 74 49 4c 24 70 fd fd 44 fd 7c 24	>D=;LD$p\AL]AH3H\$`HA_A^A]A_^]H\$LL$UVWATAUAVAWH0HM3AHHM~PHt29t$u37uD/3A7As3uAC=jHrH9OtL$pD|$	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.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 00 00 00 00 00 00 00 00 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 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd f3 34 65 00 00 00 fd fd fd fd fd fd fd fd f3 34 65 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 28 b3 34 65 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 f3 34 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 7f 00	3++S++F4e4e(4e4e	success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp.dmp	1900	48	68 06 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 60 fd 34 65 00 00 00 fd fd fd 34 65 00 00 00 08 06 00 00 fd fd 00 00 fd 04 00 00 68 35 00 00	h `4e4eh5	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.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	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.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 fd 13 13 02 00 00 fd d2 13 13 02 00 00 00 00 fd 13 13 02 00 00 3a 01 00 00 00 00 00 00 fd fd fd fd 7f 00 00 fd fd fd fd 7f 00 00 00 fd 13 13 02 00 00 1c fd fd fd 0d fd fd 01 14 10 fd 13 13 02 00 00 fd d2 13 13 02 00 00 00 00 fd 13 13 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 3a 01 00 00 00 00 00	<2|h+&BB?#`A p::	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.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 fd fd 02 00 00 00 00 fd 14 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 69 fd 00 00 00 00 00 00 06 fd 03 00 00 00 00 00 fd 66 03 00 00 00 00 00 3a fd 17 00 00 00 00 00 06 08 08 00 00 00 00 00 40 fd 1f 00 00 00 00 00 56 3a 17 00 00 00 00 00 fd fd 75 00 00 00 00 6e 46 fd 1e 00 00 00 00 fd fd 5d 21 00 00 00 00 05 fd fd 01 00 00 00 00 fd 0e 01 00 fd 1d 01 00 fd 60 07 00 fd fd 09 00 06 08 08 00 fd 1f 1a 00 56 3a 17 00 fd 2a 73 00 fd 01 00 0d fd 1d 00 00 00 00 00 0f 2e 59 00 7a fd 04 00 79 fd 00 00 00 00 00 00 00 00 00 00 09 12 00 00 39 00 00 00 70 02 00	Zbif:@V:unF]!`V:*s.Yzy9p	success or wait	1	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.tmp.dmp	59290	5236	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	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FD2.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 54 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 58 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	h8T8:`8TX!#	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 38 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3896</Pid>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 30 00 33 00 32 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>60329</Uptime>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 37 00 31 00 39 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2204204371968</PeakVirtualSize>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 38 00 33 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>197833</PageFaultCount>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1704	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1708	2	09 00		success or wait	3	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 37 00 31 00 34 00 35 00 37 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>707145728</PeakWorkingSetSize>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1814	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1818	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 33 00 33 00 39 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>793952</WorkingSetSize>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1904	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	1908	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 37 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>107784</QuotaPeakPagedPoolUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2028	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2032	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>107584</QuotaPagedPoolUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2136	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2140	2	09 00		success or wait	3	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 32 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>24280</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2270	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2274	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23928</QuotaNonPagedPoolUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2388	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2392	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 39 00 31 00 33 00 36 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>2191360</PagefileUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2474	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2478	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 33 00 32 00 33 00 38 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>802832384</PeakPagefileUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2580	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2584	2	09 00		success or wait	3	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 39 00 31 00 33 00 36 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>2191360</PrivateUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2662	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2666	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2716	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2720	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2754	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2758	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2804	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2808	2	09 00		success or wait	4	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2816	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7160</Pid>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2846	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2850	2	09 00		success or wait	4	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2930	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	2934	2	09 00		success or wait	4	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3032	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3036	2	09 00		success or wait	4	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3044	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 31 00 37 00 39 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>61791</Uptime>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3088	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3092	2	09 00		success or wait	4	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3178	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3182	2	09 00		success or wait	4	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3242	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3246	2	09 00		success or wait	4	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3298	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3302	2	09 00		success or wait	5	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 34 00 39 00 36 00 37 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>518249676768</PeakVirtualSize>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3402	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3406	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 31 00 32 00 37 00 34 00 33 00 36 00 38 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>4412743680</VirtualSize>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3490	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3494	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 32 00 30 00 30 00 35 00 38 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>200581</PageFaultCount>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3582	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3586	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 35 00 30 00 34 00 32 00 38 00 31 00 36 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>750428160</PeakWorkingSetSize>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3696	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3700	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 31 00 37 00 35 00 39 00 36 00 31 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>11759616</WorkingSetSize>	success or wait	1	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3792	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3796	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 38 00 35 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 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>202856</QuotaPeakPagedPoolUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3920	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	3924	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 35 00 30 00 37 00 39 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>150792</QuotaPagedPoolUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4032	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4036	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>11536</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4170	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4174	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 31 00 32 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>10120</QuotaNonPagedPoolUsage>	success or wait	1	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4292	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4296	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 36 00 39 00 36 00 30 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>2969600</PagefileUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4382	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4386	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4492	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4496	2	09 00		success or wait	5	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 36 00 39 00 36 00 30 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>2969600</PrivateUsage>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4578	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4582	2	09 00		success or wait	4	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4636	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4640	2	09 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4688	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4692	2	09 00		success or wait	2	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4728	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4732	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4776	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4780	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4820	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4824	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4890	4	0d 00 0a 00		success or wait	8	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	4894	2	09 00		success or wait	16	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	5554	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	5558	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	5600	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	5604	2	09 00		success or wait	1	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	5644	4	0d 00 0a 00		success or wait	6	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	5648	2	09 00		success or wait	12	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6206	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6210	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6252	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6256	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6296	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6300	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6398	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6402	2	09 00		success or wait	2	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 6e 00 62 00 63 00 6e 00 6c 00 68 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>nbcnlh, Inc.</SystemManufacturer>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6512	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6516	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 6e 00 62 00 63 00 6e 00 6c 00 68 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>nbcnlh7,1</SystemProductName>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6616	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6620	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6744	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6748	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 36 00 34 00 38 00 36 00 39 00 32 00 30 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>1616486920</OSInstallDate>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6834	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6838	2	09 00		success or wait	2	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6944	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	6948	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7020	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7024	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7066	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7070	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7106	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7110	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7210	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7214	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7252	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7256	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7282	4	0d 00 0a 00		success or wait	3	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7286	2	09 00		success or wait	6	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7536	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7540	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7568	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7572	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 30 00 3a 00 35 00 38 00 3a 00 31 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-07-22T20:58:14Z">	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7674	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7678	2	09 00		success or wait	2	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 34 00 30 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 38 00 39 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 34 00 30 00 39 00 35 00 32 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 34 00 30 00 39 00 35 00 32 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="404" PID="3896" UptimeMS="40952" TimeSinceCreationMS="40952" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7948	4	0d 00 0a 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7952	2	09 00		success or wait	6	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	7958	204	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 35 00 35 00 32 00 39 00 36 00 30 00 30 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 30 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="5529600" TimelineUnitShift="12" Timeline="10111111111111"/>	success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	8362	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	8366	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	8390	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	8394	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	8434	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	8438	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	8478	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	8482	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	8486	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 63 00 61 00 32 00 33 00 62 00 30 00 38 00 2d 00 35 00 37 00 39 00 32 00 2d 00 34 00 64 00 39 00 62 00 2d 00 38 00 64 00 65 00 39 00 2d 00 66 00 30 00 63 00 39 00 66 00 65 00 39 00 32 00 38 00 61 00 39 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>8ca23b08-5792-4d9b-8de9-f0c9fe928a98</Guid>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	8584	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	8588	2	09 00		success or wait	2	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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 30 00 3a 00 35 00 38 00 3a 00 31 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-07-22T20:58:14Z</CreationTime>	success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	8690	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	8694	2	09 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.tmp.WERInternalMetadata.xml	8736	4	0d 00 0a 00		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB5A.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	7FF8C975E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE49.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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Mlp_773949b15a9dc27bfcd3f791ccbc8dda8da3511_ceeedb37_116bd172\Report.wer	0	2	fd fd		success or wait	1	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Mlp_773949b15a9dc27bfcd3f791ccbc8dda8da3511_ceeedb37_116bd172\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	7FF8C975E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Mlp_773949b15a9dc27bfcd3f791ccbc8dda8da3511_ceeedb37_116bd172\Report.wer	9444	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 36 00 34 00 36 00 38 00 33 00 36 00 36 00 33 00	MetadataHash=2646836633	success or wait	1	7FF8C975E9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0ce580c3-9356-6b11-5fcc-934541472052}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FF8C9781D2D	unknown
\REGISTRY\A\{0ce580c3-9356-6b11-5fcc-934541472052}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FF8C9781D2D	unknown
\REGISTRY\A\{0ce580c3-9356-6b11-5fcc-934541472052}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FF8C975E3FE	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 EC 03 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 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 00 00 00 5C 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FF8C97807CB	RegSetValueExW

Analysis Process: regsvr32.exe PID: **5428**, Parent PID: **7160**

General

Target ID:	17
Start time:	13:58:11
Start date:	22/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\YbTPHZsAWIZFUi\eAeQcUPg.dll"
Imagebase:	0x7ff655380000
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: **4900**, Parent PID: **604**

General

Target ID:	20
Start time:	13:58:39
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:	0x7ff7e8070000
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

Analysis Process: svchost.exe PID: 5068, Parent PID: 604

General

Target ID:	22
Start time:	13:58:51
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:	0x7ff7e8070000
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: svchost.exe PID: 5928, Parent PID: 604

General

Target ID:	24
Start time:	13:59:10
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:	0x7ff6ec1c0000
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: 7032, Parent PID: 604

General

Target ID:	28
Start time:	13:59:32

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:	0x7ff7e8070000
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: **6188**, Parent PID: **604**

General

Target ID:	30
Start time:	13:59:44
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:	0x7ff7e8070000
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