ID: 736960
Sample Name: 5iiXyNVCQ3
Cookbook: default.jbs
Time: 12:34:10
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

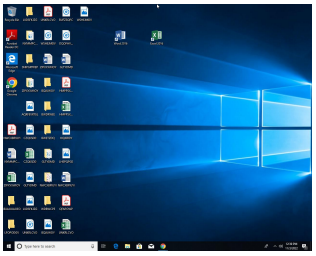
Windows Analysis Report

5iiXyNVCQ3

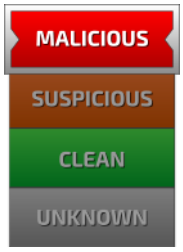
Overview

General Information

Sample Name:	5iiXyNVCQ3 (renamed file extension from none to dll)
Analysis ID:	736960
MD5:	73c06c75bd9aa0..
SHA1:	7604d4be31e6c0..
SHA256:	fde687287ef8cd7..
Infos:	



Detection

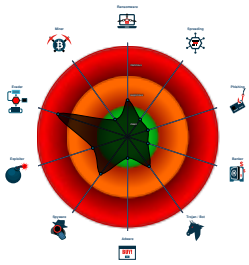


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- System process connects to networ…
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Writes to foreign memory regions
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 3144 cmdline: loaddll32.exe "C:\Users\user\Desktop\5iiXyNVCQ3.dll" MD5: 1F562FBF37040EC6C43C8D5EF619EA39)
  - conhost.exe (PID: 676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 400 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\5iiXyNVCQ3.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5996 cmdline: rundll32.exe "C:\Users\user\Desktop\5iiXyNVCQ3.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - svchost.exe (PID: 5972 cmdline: C:\WINDOWS\system32\svchost.exe -K NetworkService MD5: FA6C268A5B5BDA067A901764D203D433)
  - rundll32.exe (PID: 964 cmdline: rundll32.exe C:\Users\user\Desktop\5iiXyNVCQ3.dll,unll MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - svchost.exe (PID: 5020 cmdline: C:\WINDOWS\system32\svchost.exe -K NetworkService MD5: FA6C268A5B5BDA067A901764D203D433)
    - WerFault.exe (PID: 1372 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 964 -s 844 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - svchost.exe (PID: 3832 cmdline: C:\WINDOWS\system32\svchost.exe -K NetworkService MD5: FA6C268A5B5BDA067A901764D203D433)
  - WerFault.exe (PID: 5288 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3144 -s 616 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.rundll32.exe.475e2dd.4.unpack	MALWARE_Win_BlackMoon	Detects executables using BlackMoon RunTime	ditekSHen	• 0x5bd3b:$s1: blackmoon • 0x5bd7b:$s2: BlackMoon RunTime Error:

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.1000e2dd.1.unpack	MALWARE_Win_BlackMoon	Detects executables using BlackMoon RunTime	ditekSHen	• 0x5bd3b:$s1: blackmoon • 0x5bd7b:$s2: BlackMoon RunTime Error:
0.3.loaddll32.exe.280e2dd.0.unpack	MALWARE_Win_BlackMoon	Detects executables using BlackMoon RunTime	ditekSHen	• 0x5bd3b:$s1: blackmoon • 0x5bd7b:$s2: BlackMoon RunTime Error:
0.0.loaddll32.exe.1000e2dd.2.unpack	MALWARE_Win_BlackMoon	Detects executables using BlackMoon RunTime	ditekSHen	• 0x5bd3b:$s1: blackmoon • 0x5bd7b:$s2: BlackMoon RunTime Error:
0.2.loaddll32.exe.280e2dd.1.unpack	MALWARE_Win_BlackMoon	Detects executables using BlackMoon RunTime	ditekSHen	• 0x5bd3b:$s1: blackmoon • 0x5bd7b:$s2: BlackMoon RunTime Error:
Click to see the 12 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.48.8.8.856572532023883 11/03/22-12:35:13.698250
SID:	2023883
Source Port:	56572
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for domain / URL
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic

System Summary

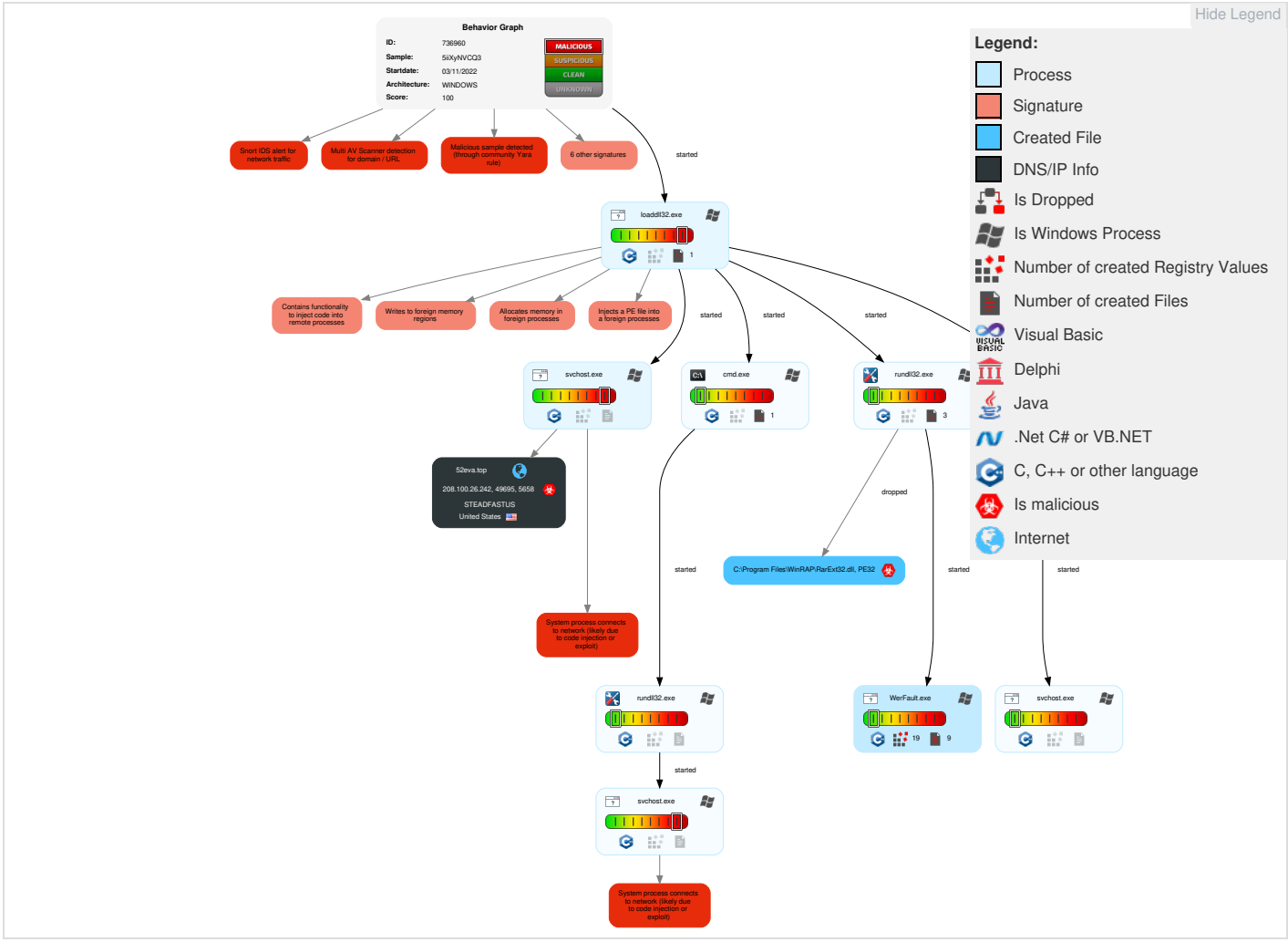
- Malicious sample detected (through community Yara rule)

System process connects to network (likely due to code injection or exploit)
Writes to foreign memory regions
Allocates memory in foreign processes
Injects a PE file into a foreign processes
Contains functionality to inject code into remote processes

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	1 Native API	Path Interception	5 1 1 Process Injection	1 Deobfuscate/Decode Files or Information	1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	4 Obfuscated Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Software Packing	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	2 Clipboard Data	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Masquerading	NTDS	1 3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Virtualization/Sandbox Evasion	LSA Secrets	1 1 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	5 1 1 Process Injection	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	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 Rundll32	DCSync	2 Process 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	Indicator Removal from Tools	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Owner/User 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)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

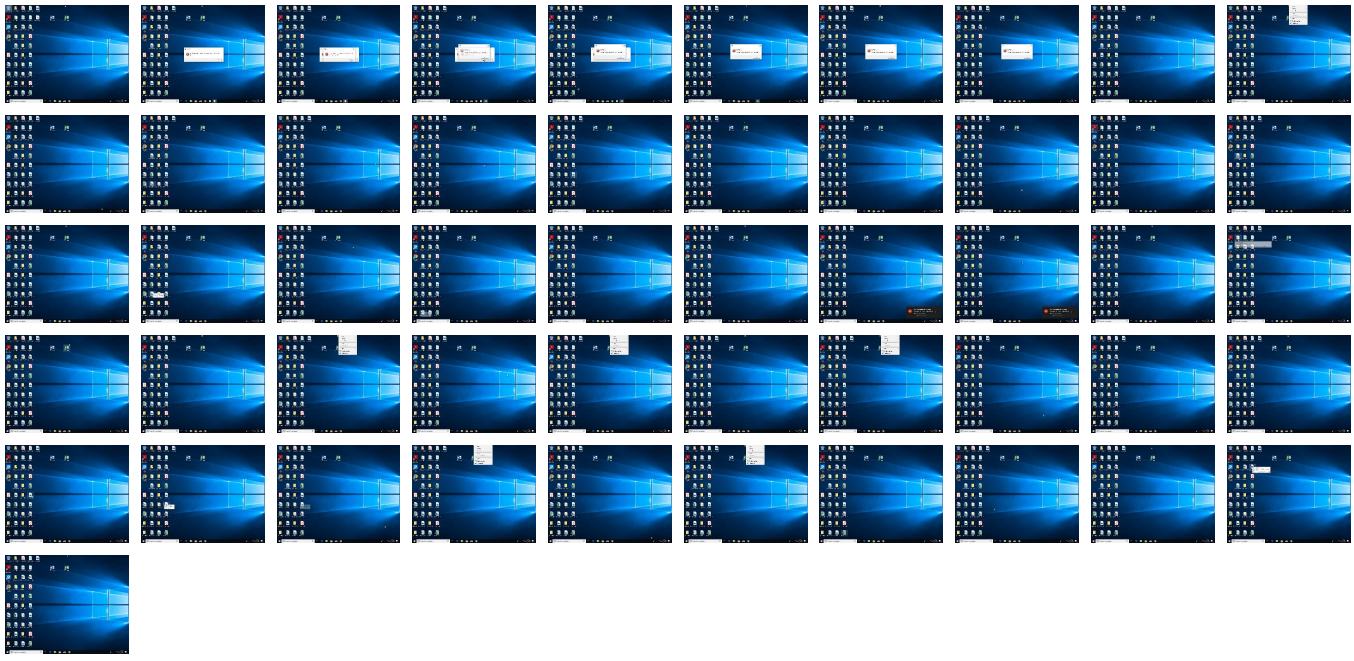
Behavior Graph



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
5iiXyNVCQ3.dll	93%	Virustotal		Browse
5iiXyNVCQ3.dll	95%	ReversingLabs	Win32.Trojan.Qqblack	
5iiXyNVCQ3.dll	80%	Metadefender		Browse
5iiXyNVCQ3.dll	100%	Avira	HEUR/AGEN.1238485	
5iiXyNVCQ3.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files\WinRAP\RarExt32.dll	100%	Avira	HEUR/AGEN.1238485	
C:\Program Files\WinRAP\RarExt32.dll	100%	Joe Sandbox ML		
C:\Program Files\WinRAP\RarExt32.dll	95%	ReversingLabs	Win32.Trojan.Qqblack	
C:\Program Files\WinRAP\RarExt32.dll	93%	Virustotal		Browse
C:\Program Files\WinRAP\RarExt32.dll	80%	Metadefender		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.loaddll32.exe.bd4498.0.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
0.0.loaddll32.exe.280e2dd.4.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
3.0.rundll32.exe.1000e2dd.2.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
3.0.rundll32.exe.475e2dd.1.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
7.3.svchost.exe.e56000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.loaddll32.exe.280e2dd.0.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
0.0.loaddll32.exe.1000e2dd.2.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
0.2.loaddll32.exe.280e2dd.1.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
3.0.rundll32.exe.475e2dd.4.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
4.2.rundll32.exe.1000e2dd.1.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
3.2.rundll32.exe.f1fe88.0.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
3.2.rundll32.exe.475e2dd.1.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
3.3.rundll32.exe.475e2dd.0.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
4.3.rundll32.exe.68ffa0.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.3.svchost.exe.eab008.0.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
4.3.rundll32.exe.aee2dd.0.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
3.0.rundll32.exe.1000e2dd.5.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
3.0.rundll32.exe.f1fe88.3.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
0.0.loaddll32.exe.1000e2dd.5.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
3.0.rundll32.exe.f1fe88.0.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
7.2.svchost.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1225179		Download File
0.0.loaddll32.exe.bd4498.3.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
0.2.loaddll32.exe.1000e2dd.2.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
4.2.rundll32.exe.aee2dd.0.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
3.2.rundll32.exe.1000e2dd.2.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
0.0.loaddll32.exe.280e2dd.1.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File
4.3.rundll32.exe.68ffa0.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.loaddll32.exe.bd4498.0.unpack	100%	Avira	TR/Crypt.NSPM.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
52eva.top	7%	Virustotal		Browse

URLs

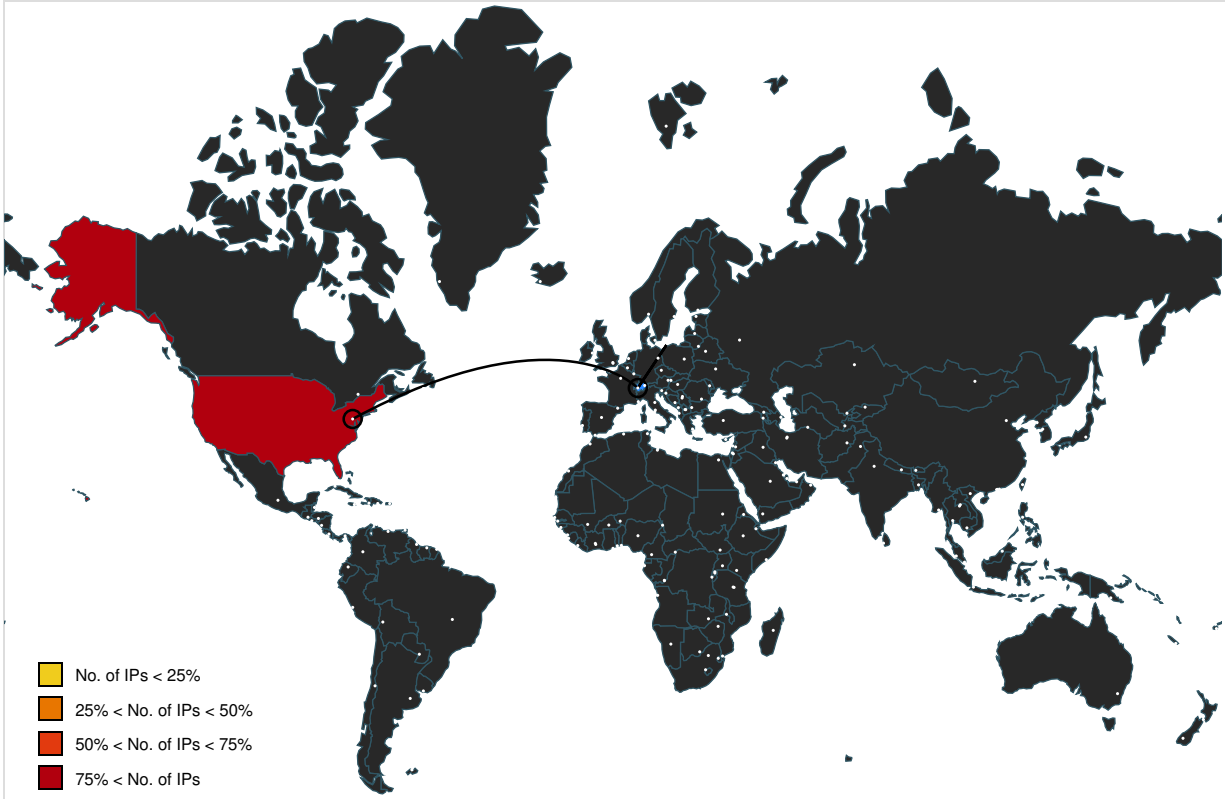
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
52eva.top	208.100.26.242	true	true	• 7%, Virustotal, Browse	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.100.26.242	52eva.top	United States		32748	STEADFASTUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736960
Start date and time:	2022-11-03 12:34:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5iiXyNVCQ3 (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 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.evad.winDLL@16/9@1/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 24.3% (good quality ratio 23.4%) • Quality average: 81.5% • Quality standard deviation: 25.2%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.20, 20.42.73.29
- Excluded domains from analysis (whitelisted): login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, onedsblobprdwus15.westus.cloudapp.azure.com, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:35:13	API Interceptor	1x Sleep call for process: loaddll32.exe modified
12:35:19	API Interceptor	2x Sleep call for process: WerFault.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:\Program Files\WinRAP\RarExt32.dll

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	346783
Entropy (8bit):	**7.996288147606643**
Encrypted:	**true**
SSDEEP:	6144:nuPt5aWk+Y/3hINHl9bVKRI0cZ+rmSM2DTIMVfPshRkj7ITKWVE3Rr1BdFnIi3Dq:nq5ayQRIBPQpx4MKVfPcEMeW4r1r1q2Q
MD5:	73C06C75BD9AA0A194B0DC73AB38CAC5
SHA1:	7604D4BE31E6C017E3BD9A1E5590A81A7AAFB40F
SHA-256:	FDE687287EF8CD7E6A6CE655355EACA2FBA25FD6C22CC1E4040281F73205BA90
SHA-512:	C8ABAEA48ABC45FDB8C20EE1945494C42E0E3CD487723F48BD34F31FD31833A94DEB38796397C8359FB3123E028A99AB5E8E05438399DCC34AE65D522F78487A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 95% • Antivirus: Virustotal, Detection: 93%, Browse • Antivirus: Metadefender, Detection: 80%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .L`N.L`N.L`N.7|B.M`N.o..N`N..|@.N`N.#.J.N`N..D.N`N.L`O."`N.o.._`N.zFE.z`N.L`N.M`N..E.O`N..J.M`N.RichL`N.....PE..L.....bX.....!.....P... ..N5.....0.....f>..>....3.....0.....>.....nsp0.... .....`....nsp1....P...0...F.....`....nsp2...G.....`.....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_9cdbf19a94ecdea39c14ee8fd4f9ea7f9e7533d_fe4ae974_14fd8b6a\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8400335209117962
Encrypted:	false
SSDEEP:	96:89rfFEagpyMy9hy1Dg/jSupXIQcQ8c6+RccEmcw3G+a+z+HbHg/cBRTf3ocFa9ic:8hD7HSq6MYjAD/u7sfS274ltb
MD5:	029B56FA46932336D4C61BCBFC7C378F
SHA1:	C669704DC882324B11DB6C3522B1E55A873DC56C
SHA-256:	5E4A1C71BAE91320F892346A7B9FC2414CB7F3B027845718669602496755182B
SHA-512:	496C8F34DDAECE907A9880EB3ECF94582261112687BFEE45C4880FE41D5B76F7982D703F07C4BEC5EC839FFC09BDD1561EAD706117AE7326FA922CD1FB68575
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.1.1.9.4.8.9.1.6.2.3.2.3.9.0.9.....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.=.1.3.3.1.1.9.4.8.9.1.7.5.9.1.7.6.4.2.....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.=.c.b.7.0.b.6.e.3.-.c.5.2.f.-.4.f.c.4.-.9.1.d.3.-.e.c.e.2.e.1.a.f.8.3.c.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.=.4.5.4.5.f.7.5.1.-.4.2.1.4.-.4.7.5.3.-.9.6.0.b.-.7.2.f.8.3.e.9.2.b.a.f.1.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.0.c.4.8.-.0.0.0.1.-.0.0.1.f.-.7.e.8.a.-.c.f.5.3.7.8.e.f.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_69aa54bf4562ff7e548e4d05abc368941456d4_82810a17_050990c9\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9541844269298931
Encrypted:	false
SSDEEP:	192:5OoziG0oXQHrCiljed+v/u7sfS274lt7c:AozigX4rCiljei/u7sfX4lt7c
MD5:	D4871BD5F09D001ED088F83000470E6C
SHA1:	FFCAB51A20C499035AE146931589B1FD9E9FD4E1
SHA-256:	31F9341886D4BC84A223453E44A5EA72581C1FE8553125FC413B9BB4918DEDD4

SHA-512:	DBBA522DEE9296ADB9E1A475903AB3738D538D26A66E688AE006F8426F19987CFE39CA59278591DF1B9DD88B9FE7A08D9D09DBB49A211BD3478715E894800605
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.1.1.9.4.8.9.1.8.2.6.4.0.9.6.9.....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.=.1.3.3.1.1.9.4.8.9.1.9.7.1.7.2.2.0.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.5.c.b.7.1.7.e.-.f.7.0.a.-.4.7.1.d.-.9.0.7.1.-.5.4.b.7.e.f.9.6.1.e.6.5.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.9.6.d.9.e.b.d.-.7.0.6.6.-.4.5.f.d.-.9.e.a.a.-.b.5.b.6.5.2.c.4.c.e.7.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....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.=.0.0.0.0.0.3.c.4.-.0.0.0.1.-.0.0.1.f.-.1.3.3.3.-.0.9.5.4.7.8.e.f.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.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Nov 3 11:35:16 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	52196
Entropy (8bit):	2.100276099272835
Encrypted:	false
SSDEEP:	384:M5/e3Pu10D2Mc31XAU7gB4PxVTnaRsjX9e:A/e3PQXAU7gBEVrH9e
MD5:	EB05BCAEF80D6506CB224436AABDF23B
SHA1:	B7C399B3652175ED0C13349064A4CF82B73C046E
SHA-256:	BDB78C5C68739527F64F8F5E4D02722E7EA16A59BBD7D51F06ABF43325A2F24D
SHA-512:	936320A6FF6E732E18C93E04C5B05D50F7B70B34AB4C9635D34736AC5C4C352CF0E136081159EBCCEC17F523274BF70E57AA8111F379CCFD281B09C6FEE9229C
Malicious:	false
Preview:	MDMP..... .....t.cc.....<.....4....+.....`.....8.....T.....U.....B.....`..... ..GenuineIntelW.....T.....H...I.cc.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8362
Entropy (8bit):	3.6863479858171404
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNigz6r7Xc6YeCSUD0gmf+RSyiQ+pDN89baIsfSem:RrlsNiU6r7Xc6Y7SUD0gmf+RSyVa7fi
MD5:	DFAD9C1AB9D806D7B01DDAFAF8ACD34B
SHA1:	59C0AD8ACF214B2EC64EDB2751E98CC159245C4F
SHA-256:	D8CF1907D1E9B46F8EE1D90E6377FEFFF34A6C16582A972DCD1BFF26AAC5773E
SHA-512:	FF618E82D4383B86F4B4890346DDC2A6560574049B129190433E860FBA7C2F18C6F2F9E50E035282AF48344E144C4A6E91F422AFF04B1290842E6A9112DB99DB
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.>.3.1.4.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER83CA.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4659
Entropy (8bit):	4.417019346367334
Encrypted:	false
SSDEEP:	48:cvIwSD8zsEJgtWI9vvWgc8sqYjU8fm8M4JtNJF1x+q8vvNzKcQIcQwj4d:uITfCI+grsqY9JjKNKkwj4d
MD5:	2458C14FABB503C2EC5BB679358ACBD3
SHA1:	590750A58C4B7D08D8C7FE6982917D1BAB14D0AD
SHA-256:	8FD99E797CDF7937C7E653E9AD6B551FABBE95EDF2CB2EF18F67EF9CD202844D
SHA-512:	A83B9728E50562E8BF64A8FC9A85B9D56C0325C70AE47A7743B6182E11D29DB0FACBABC37225D107561232D97C972C599234E24221E2111D1D73AE1461811A9(
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="1763805" />.. <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\WER885C.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Nov 3 11:35:18 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	54232
Entropy (8bit):	2.031946433338903
Encrypted:	false
SSDEEP:	192:1S5RU7kxSJ1O5SkbJYh0aKyiM2PDdAQtnq/v8wYVuedFZCATN3cm:qxF5Lb002J2PDdAQQYVuy3Nsm
MD5:	AA44E92E0176A2ACF98F8858692C0ABD
SHA1:	E9BDE845E0E90E3192DFA6783BB156990C18928A
SHA-256:	17232689A5E7C9B99F13C02CD1ED79D7AB4A9414B95E3EF370C1D5EDD10EBAEB
SHA-512:	4DD89C5418B9D451B5B5A7C3F1CF7B12896271731D551D6623007BF1770E81F2165095971E5C4C07C0BDD50D2B831E6A1207D74FAA28463ABDA40F71DC864C7
Malicious:	false
Preview:	MDMP..... .....v.cc.....$.....t....3.....`.....8.....T.....!.....U.....B..... ...GenuineIntelW.....T.....m.cc.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8346
Entropy (8bit):	3.6859501652550146
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiGN60zl66YgD067b/Mgmf8kRSKQ+pDH89bd0sfYfm:RrlsNic696Yq067b/Mgmf8kRS/dnfN
MD5:	80A5435F92AC764FD43A4D26D0F6A498
SHA1:	5EE6E7A91C9586B919A870876DC2279EAD34A071
SHA-256:	227B42D87F9C480DC3373FD2FA6DFF47CF3BC75DFFAB293D8B51A4CE7A778BB8
SHA-512:	7DB8567B178598F64A7E32428578D55C7C9DA6F6A084A5468701F47D15D3B11597BAAD31DA5BAC9EE7D6F4FBA38DB2F5739E855C685EE7D856B07ED82B5DA38
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.>.9.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C46.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4731
Entropy (8bit):	4.438037024201743
Encrypted:	false
SSDEEP:	48:cvIwSD8zsEJgtWI9vvWgc8sqYjU8fm8M4JCdsNJFuDo+q8vjsNLA4SrSKd:uITfCI+grsqYlJwoKkADWKd
MD5:	C3E1CAEDBAABCB26F01B8D4816EAA26E
SHA1:	CBB46BBC8F6DD48E9BE7836B93512ED62F541225
SHA-256:	E7C3546CE9687DA3F667E49464BBACA4514BE6A1145C2C202B1D143B70E71CCD
SHA-512:	C822A0B7AE5BE0256C50D4084036B6541CD09B271BA0E75E8CBD8F1B0F0F97C484B518A7B713582FB0B4B840C4540FAEFDE2568B8D342BD0CD044134ABD011A
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="1763805" />.. <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" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.996288147606643
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	5iiXyNVCQ3.dll
File size:	346783
MD5:	73c06c75bd9aa0a194b0dc73ab38cac5
SHA1:	7604d4be31e6c017e3bd9a1e5590a81a7aafb40f
SHA256:	fde687287ef8cd7e6a6ce655355eaca2fba25fd6c22cc1e4040281f73205ba90
SHA512:	c8abaea48abc45fdb8c20ee1945494c42e0e3cd487723f48bd34f31fd31833a94deb38796397c8359fb3123e028a99ab5e8e05438399dcc34ae65d522f78487a
SSDEEP:	6144:nuPt5aWk+Y/3hINHl9bVKRI0cZ+rmSM2DTIMVfPshRkj7ITKWVE3Rr1BdFnIi3Dq:nq5ayQRIBPQpx4MKVfPcEMeW4r1r1q2Q
TLSH:	B174229DD43BBC04C24357F491121B930F57BD5CDAA2206572FE2DF6881AE205FB2EA6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .L`N.L`N.L`N.7|B.M`N..o..N`N..|@.N`N.#.J.N`N...D.N`N.L`O."`N..o.._`N.zFE.z`N.L`N.M`N...E.O`N...J.M`N.RichL`N.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1008354e
Entrypoint Section:	.nsp1
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, DLL
DLL Characteristics:	
Time Stamp:	0x5862801B [Tue Dec 27 14:52:11 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	99eb8dcfbd1a7e02dc8bf9d49c4aa67c

Entrypoint Preview

Instruction
pushfd
pushad
call 00007F9124999295h
pop ebp

Instruction
mov eax, 00000007h
sub ebp, eax
lea esi, dword ptr [ebp-00000272h]
mov al, byte ptr [esi]
cmp al, 00h
je 00007F91249992A4h
mov esi, ebp
lea esi, dword ptr [ebp-0000024Ah]
mov al, byte ptr [esi]
cmp al, 01h
je 00007F91249994D8h
mov byte ptr [esi], 00000001h
mov edx, ebp
sub edx, dword ptr [ebp-000002B6h]
mov dword ptr [ebp-000002B6h], edx
add dword ptr [ebp-00000286h], edx
lea esi, dword ptr [ebp-00000242h]
add dword ptr [esi], edx
pushad
push 00000040h
push 00001000h
push 00001000h
push 00000000h
call dword ptr [ebp-0000020Eh]
test eax, eax
je 00007F9124999600h
mov dword ptr [ebp-0000028Eh], eax
call 00007F9124999295h
pop ebx
mov ecx, 00000368h
add ebx, ecx
push eax
push ebx
call 00007F9124999546h
popad
mov esi, dword ptr [esi]
mov edi, ebp
add edi, dword ptr [ebp-000002C6h]
mov ebx, edi
cmp dword ptr [edi], 00000000h
jne 00007F912499929Ch
add edi, 04h
mov ecx, 00000000h
jmp 00007F91249992A8h
mov ecx, 00000001h
add edi, dword ptr [ebx]
add ebx, 04h
cmp dword ptr [ebx], 00000000h
je 00007F91249992C8h
add dword ptr [ebx], edx
mov esi, dword ptr [ebx]
add edi, dword ptr [ebx+04h]
push edi
push ecx
push edx
push ebx
push dword ptr [ebp-0000020Ah]
push dword ptr [ebp-0000020Eh]
mov edx, esi

Rich Headers

Programming Language:	• [C] VS98 (6.0) build 8168 • [C++] VS98 (6.0) SP6 build 8804 • [C++] VS98 (6.0) build 8168 • [LNK] VS98 (6.0) imp/exp build 8168

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x83e66	0x3e	.nsp1
IMAGE_DIRECTORY_ENTRY_IMPORT	0x83380	0xa0	.nsp1
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x83000	0x288	.nsp1
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x83ea4	0x8	.nsp1
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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
.nsp0	0x1000	0x82000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.nsp1	0x83000	0x55000	0x5469f	False	0.9981345387972548	data	7.998366920306635	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.nsp2	0xd8000	0x1747	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x83058	0x230	data	Chinese	China

Imports

DLL	Import
KERNEL32.DLL	LoadLibraryA, GetProcAddress, VirtualProtect, VirtualAlloc, VirtualFree, ExitProcess
USER32.DLL	DispatchMessageA
ADVAPI32.DLL	RegCloseKey
WS2_32.DLL	WSAStartup
SHLWAPI.DLL	PathFileExistsA
MSVCRT.DLL	??3@YAXPAX@Z
SHELL32.DLL	SHGetSpecialFolderPathA

Exports

Name	Ordinal	Address
unll	1	0x10008e14

Possible Origin

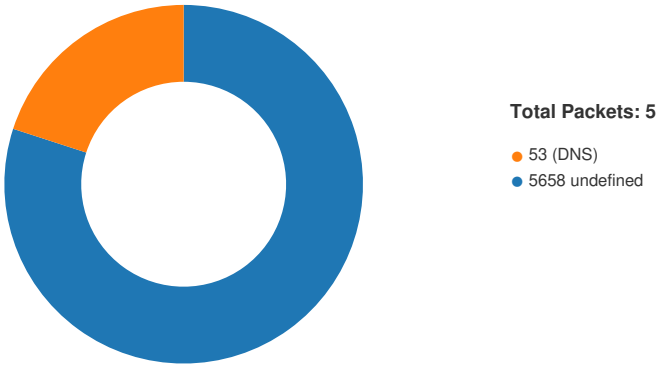
Language of compilation system	Country where language is spoken	Map
Chinese	China	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.48.8.8.8.8565725 32023883 11/03/22-12:35:13.698250	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	56572	53	192.168.2.4	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:35:14.111439943 CET	49695	5658	192.168.2.4	208.100.26.242
Nov 3, 2022 12:35:14.234112024 CET	5658	49695	208.100.26.242	192.168.2.4
Nov 3, 2022 12:35:14.234241962 CET	49695	5658	192.168.2.4	208.100.26.242
Nov 3, 2022 12:35:14.356290102 CET	5658	49695	208.100.26.242	192.168.2.4
Nov 3, 2022 12:35:14.356889009 CET	49695	5658	192.168.2.4	208.100.26.242
Nov 3, 2022 12:35:14.448417902 CET	49695	5658	192.168.2.4	208.100.26.242
Nov 3, 2022 12:35:14.570745945 CET	5658	49695	208.100.26.242	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:35:13.698250055 CET	56572	53	192.168.2.4	8.8.8.8
Nov 3, 2022 12:35:14.096695900 CET	53	56572	8.8.8.8	192.168.2.4

DNS Queries

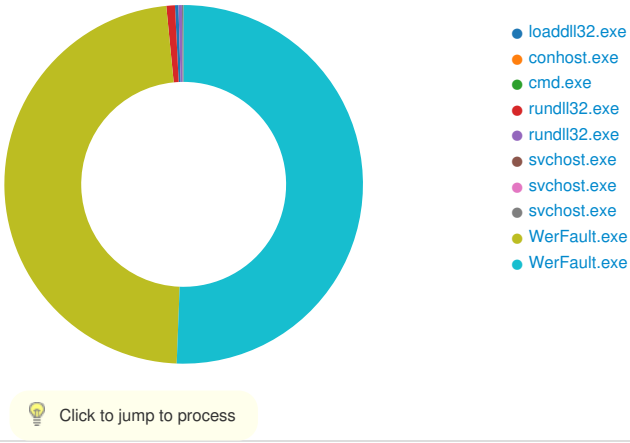
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 3, 2022 12:35:13.698250055 CET	192.168.2.4	8.8.8.8	0xdf81	Standard query (0)	52eva.top	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 3, 2022 12:35:14.096695900 CET	8.8.8.8	192.168.2.4	0xdf81	No error (0)	52eva.top		208.100.26.242	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 3144, Parent PID: 3528

General

Target ID:	0
Start time:	12:35:08
Start date:	03/11/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\5iiXyNVCQ3.dll"
Imagebase:	0x1230000
File size:	116736 bytes
MD5 hash:	1F562FBF37040EC6C43C8D5EF619EA39
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Analysis Process: conhost.exe PID: 676, Parent PID: 3144

General

Target ID:	1
Start time:	12:35:09
Start date:	03/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **400**, Parent PID: **3144**

General

Target ID:	2
Start time:	12:35:09
Start date:	03/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\5iiXyNVCQ3.dll",#1
Imagebase:	0xd90000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: rundll32.exe PID: **964**, Parent PID: **3144**

General

Target ID:	3
Start time:	12:35:09
Start date:	03/11/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\5iiXyNVCQ3.dll,unll
Imagebase:	0x1120000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	10002F81	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files\WinRAP	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	10002F81	CreateDirectoryA
C:\Program Files\WinRAP\RarExt32.dll	write data or add file | read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	10003093	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\WinRAP\RarExt32.dll	0	346783	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 08 01 20 fd 4c 60 4e fd 4c 60 4e fd 4c 60 4e fd 37 7c 42 fd 4d 60 4e 8f 6f 11 fd 4e 60 4e fd fd 7c 40 fd 4e 60 4e fd 23 7f 4a fd 4e 60 4e a4 7f 44 fd 4e 60 4e fd 4c 60 4f fd 22 60 4e 8f 6f 13 fd 5f 60 4e fd 7a 46 45 fd 7a 60 4e fd 4c 60 4e fd 4d 60 4e a4 7f 45 fd 4f 60 4e a4 7f 4a fd 4d 60 4e fd 52 69 63 68 4c 60 4e fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$ L`NL`NL`N7|BM `NoN`N|@N`N#JN`NDN`NL`O"`No_`N zFEz`NL`NM`NEO`NJM` NRichL`N	success or wait	1	10003254	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\5iiXyNVCQ3.dll	unknown	346783	success or wait	1	100096FE	ReadFile

Analysis Process: rundll32.exe PID: **5996**, Parent PID: **400**

General

Target ID:	4
Start time:	12:35:09
Start date:	03/11/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\5iiXyNVCQ3.dll",#1
Imagebase:	0x1120000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	346783			invalid handle	1	10003254	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\5iiXyNVCQ3.dll	unknown	346783	success or wait	1	100096FE	ReadFile

Analysis Process: svchost.exe PID: **5972**, Parent PID: **5996**

General

Target ID:	5
Start time:	12:35:09
Start date:	03/11/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\WINDOWS\system32\svchost.exe -K NetworkService
Imagebase:	0x12b0000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **5020**, Parent PID: **964**

General

Target ID:	6
Start time:	12:35:09
Start date:	03/11/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\WINDOWS\system32\svchost.exe -K NetworkService
Imagebase:	0x12b0000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **3832**, Parent PID: **3144**

General

Target ID:	7
Start time:	12:35:12
Start date:	03/11/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\WINDOWS\system32\svchost.exe -K NetworkService
Imagebase:	0x12b0000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true

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

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WinRAP\RarExt32.dll	unknown	346783	success or wait	1	483B01	ReadFile

Analysis Process: WerFault.exe PID: **5288**, Parent PID: **3144**

General

Target ID:	10
Start time:	12:35:15
Start date:	03/11/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3144 -s 616
Imagebase:	0xb50000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
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	6D5B1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83CA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83CA.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_9cdbf19a94ecdea39c14ee8fd4f9ea7f9e7533d_fe4ae974_14fd8b6a	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_9cdbf19a94ecdea39c14ee8fd4f9ea7f9e7533d_fe4ae974_14fd8b6a\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D5A497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83CA.tmp	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83CA.tmp.xml	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8407.tmp.csv	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8531.tmp.txt	success or wait	1	6D5A497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	0	32	4d 44 4d 50 fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 74 fd 63 63 fd 05 12 00 00 00 00 00	MDMP tcc	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	6496	6	00 00 00 00 00 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 60 19 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 48 0c 00 00 6c fd 63 63 00 00 00 00 00 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 01 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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	UB`GenuineIntelWTHlcc0 W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	7602	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 4c 5b fd 00 38 fd fd 00 03 00 00 00 08 5b fd 00 00 fd fd 00 13 03 fd 77 23 00 00 00 02 02 00 00 fd fd fd 00 2b 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 fd fd fd fd fd fd fd fd fd fd fd	?+S++L[8[w#+	success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	1632	168	58 12 00 00 00 00 00 00 09 04 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 13 03 fd 77 00 00 00 00 01 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 02 00 00 fd 1d 00 00	Xw	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	11182	20	13 00 00 00 fd fd fd 00 00 00 00 00 60 08 00 00 fd 2c 00 00	`,	success or wait	19	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	11490	2144	fd fd fd 77 fd fd fd 77 fd 00 00 00 fd fd fd fd 10 00 00 00 34 fd fd 00 00 fd fd 00 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd 00 40 fd 00 00 40 fd 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 40 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd 19 fd 00 00 00 00 00 00 00 00 00 fd fd fd 00 00 fd fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 3c fd 17 01 54 fd 00 44 fd 17 01 fd fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ww4@w@w@@@<TD	success or wait	18	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	40894	256	fd 04 00 fd fd 03 10 04 00 fd 10 78 fd 76 fd fd fd 04 00 fd fd 04 10 00 00 fd 10 78 fd 76 fd fd fd 14 00 fd fd 05 10 00 00 fd 10 78 fd 76 fd fd fd 08 00 fd fd 06 10 03 00 fd 10 78 fd 76 fd fd fd 04 00 fd fd 07 10 0c 00 fd 10 78 fd 76 fd fd fd 0c 00 fd fd 08 10 00 00 fd 10 78 fd 76 fd fd fd 04 00 fd fd 09 10 00 00 fd 10 78 fd 76 fd fd fd 10 00 fd fd 0a 10 00 00 fd 10 78 fd 76 fd fd fd 1c 00 fd fd 0b 10 00 00 fd 10 78 fd 76 fd fd fd 2c 00 fd fd 0c 10 03 00 fd 10 78 fd 76 fd fd fd 04 00 fd fd 0d 10 03 00 fd 10 78 fd 76 fd fd fd 04 00 fd fd 0e 10 07 00 fd 10 78 fd 76 fd fd fd 08 00 fd fd 0f 10 01 00 fd 10 78 fd 76 fd fd cd 49 00 fd 10 10 00 00 fd 10 78 fd 76 fd fd fd 08 00 fd fd 11 10 00 00 fd 10 78 fd 76 fd fd fd 08 00 fd fd 12 10 00 00 fd 10 78 fd 76 fd	xvxvxvxvxvxvxvxvxv,xvxvxvxvlxvxvxv	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	1800	4	04 00 00 00		success or wait	4	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	8318	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 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 fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 08 5b fd 00 00 fd fd 00 13 03 fd 77 23 00 00 00 02 02 00 00 fd fd fd 00 2b 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 fd fd fd fd fd fd fd fd fd fd fd	?+S++[w#+	success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	1948	48	fd 12 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 24 fd 02 00 00 00 00 fd 16 00 00 36 fd 00 00 fd 02 00 00 fd 28 00 00	$6(	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	2008	4	23 00 00 00	#	success or wait	35	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	6502	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	loaddll32.exe	success or wait	35	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	5684	120	00 00 40 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 54 1d 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 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	@t0Us@TBB?#@A	success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	7534	34	1c 00 00 00 35 00 69 00 69 00 58 00 79 00 4e 00 56 00 43 00 51 00 33 00 2e 00 64 00 6c 00 6c 00 00 00	5iiXyNVCQ3.dll	success or wait	2	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	5828	668	00 00 00 10 00 00 00 00 00 fd 0d 00 00 00 00 00 00 00 00 00 fd 1d 00 00 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 7f 00 00 00 00 0f 00 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 10 03 03 00 00 00 00 fd 4d 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 44 76 03 00 00 00 00 00 0a 79 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 47 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 04 00 00 00 00 00 00 fd 03 13 7b 00 00 00 00 17 fd fd 17 00 00 00 00 d8 44 10 00 00 00 00 00 4d 49 7b 01 00 00 00 00 00 fd fd 00 00 1f fd 00 00 4b fd 05 00 fd 0d 0b 00 fd fd 04 00 06 fd 1f 00 fd fd 04 00 7c 33 22 00 01 25 01 00 fd fd 0e 00 00 00 00 00 4b 5e 13 00 fd 68 04	ZbMDvyG@{DMI{K|3"%K ^h	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	41150	11046	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER806D.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0e 00 00 fd 07 00 00 0e 00 00 00 3c 00 00 00 fd 16 00 00 05 00 00 00 34 01 00 00 fd 2b 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 08 1c 00 00 2f 00 00 15 00 00 00 fd 01 00 00 fd 16 00 00 16 00 00 00 fd 00 00 00 fd 18 00 00	<4+`8T	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3144</Pid>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1002	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 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>loaddll32.exe</ImageName>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1082	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1180	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 30 00 37 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>8070</Uptime>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1230	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1320	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1380	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1434	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 30 00 33 00 39 00 35 00 33 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>110395392</PeakVirtualSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1532	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 30 00 32 00 31 00 34 00 34 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>105021440</VirtualSize>	success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1604	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1608	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1614	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 31 00 37 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>3173</PageFaultCount>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1688	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1692	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1698	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 30 00 34 00 35 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>10604544</PeakWorkingSetSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1796	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1800	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1806	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 30 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>10604544</WorkingSetSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1888	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1892	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	1898	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 34 00 39 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>249544</QuotaPeakPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2012	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2016	2	09 00		success or wait	3	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2022	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 30 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>239048</QuotaPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2120	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2124	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2130	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 31 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>40112</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2254	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2258	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2264	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 39 00 39 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>39976</QuotaNonPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2372	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2376	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2382	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 32 00 35 00 31 00 36 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4251648</PagefileUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2458	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2462	2	09 00		success or wait	3	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2468	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 32 00 35 00 35 00 37 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>4255744</PeakPagefileUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2560	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2564	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2570	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 32 00 35 00 31 00 36 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4251648</PrivateUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2642	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2646	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2650	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2696	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2700	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2704	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2734	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2738	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2744	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2784	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2788	2	09 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2796	30	3c 00 50 00 69 00 64 00 3e 00 33 00 35 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3528</Pid>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2826	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2830	2	09 00		success or wait	4	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2838	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2908	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2912	2	09 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	2920	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3010	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3014	2	09 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3022	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 36 00 30 00 33 00 37 00 35 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5603753</Uptime>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3070	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3074	2	09 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3082	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3160	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3164	2	09 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3172	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3224	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3228	2	09 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3236	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	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3280	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3284	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3294	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3384	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3388	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3398	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3472	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3476	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3486	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 30 00 37 00 38 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>60788</PageFaultCount>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3562	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3566	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3576	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 38 00 38 00 38 00 36 00 34 00 30 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>118886400</PeakWorkingSetSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3676	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3680	2	09 00		success or wait	5	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3690	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 38 00 38 00 32 00 39 00 30 00 35 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>118829056</WorkingSetSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3774	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3778	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3788	116	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 31 00 34 00 32 00 36 00 31 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>1142616</QuotaPeakPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3904	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3908	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	3918	100	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 39 00 36 00 34 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1096480</QuotaPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4018	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4022	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4032	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 37 00 36 00 30 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>87600</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4156	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4160	2	09 00		success or wait	5	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4170	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 32 00 32 00 30 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>82208</QuotaNonPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4278	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4282	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4292	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 32 00 38 00 31 00 38 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>44281856</PagefileUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4370	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4374	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4384	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 36 00 34 00 35 00 38 00 32 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>45645824</PeakPagefileUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4478	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4482	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4492	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 32 00 38 00 31 00 38 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>44281856</PrivateUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4566	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4570	2	09 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4578	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4624	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4628	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4634	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4676	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4680	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4684	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4716	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4720	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4722	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4764	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4768	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4770	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4808	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4812	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4816	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4868	4	0d 00 0a 00		success or wait	9	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4872	2	09 00		success or wait	18	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	4876	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>loaddll32.exe</Parameter0>	success or wait	9	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	5552	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	5556	2	09 00		success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	5558	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	5598	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	5602	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	5604	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	5642	4	0d 00 0a 00		success or wait	6	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	5646	2	09 00		success or wait	12	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	5650	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6204	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6208	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6210	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6250	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6254	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6256	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6294	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6298	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6302	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6396	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6400	2	09 00		success or wait	2	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6404	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 65 00 6a 00 79 00 65 00 73 00 6c 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>ejyesl, Inc.</SystemManufacturer>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6510	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6514	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6518	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 65 00 6a 00 79 00 65 00 73 00 6c 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>ejyesl7,1</SystemProductName>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6614	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6618	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6622	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6742	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6746	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6750	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 32 00 37 00 32 00 38 00 38 00 33 00 35 00 39 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>1627288359</OSInstallDate>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6840	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6942	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6946	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	6950	70	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 2d 00 30 00 31 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>-01:00</TimeZoneBias>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7020	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7024	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7066	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7070	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7106	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7110	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7210	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7214	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7252	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7256	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7282	4	0d 00 0a 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7286	2	09 00		success or wait	6	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7290	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>80000000</Flags>	success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7536	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7540	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7568	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7572	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.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 31 00 31 00 2d 00 30 00 33 00 54 00 31 00 31 00 3a 00 33 00 35 00 3a 00 31 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-03T11:35:16Z">	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7674	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7678	2	09 00		success or wait	2	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7682	262	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 32 00 39 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 31 00 34 00 34 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 32 00 39 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 32 00 39 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="291" PID="3144" UptimeMS="4296" TimeSinceCreationMS="4296" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7952	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7972	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7976	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	7978	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	8016	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	8020	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	8022	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	8060	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	8064	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	8068	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 62 00 37 00 30 00 62 00 36 00 65 00 33 00 2d 00 63 00 35 00 32 00 66 00 2d 00 34 00 66 00 63 00 34 00 2d 00 39 00 31 00 64 00 33 00 2d 00 65 00 63 00 65 00 32 00 65 00 31 00 61 00 66 00 38 00 33 00 63 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>cb70b6e3-c52f-4fc4-91d3-ece2e1af83c9</Guid>	success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	8166	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	8170	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	8174	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 31 00 31 00 2d 00 30 00 33 00 54 00 31 00 31 00 3a 00 33 00 35 00 3a 00 31 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-11-03T11:35:16Z</CreationTime>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	8272	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	8276	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	8278	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	8318	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER832D.tmp.WERInternalMetadata.xml	8322	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER83CA.tmp.xml	0	4659	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 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_9cdbf19a94ecdea39c14ee8fd4f9ea7f9e7533d_fe4ae974_14fd8b6a\Report.wer	0	2	fd fd		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_9cdbf19a94ecdea39c14ee8fd4f9ea7f9e7533d_fe4ae974_14fd8b6a\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	162	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_9cdbf19a94ecdea39c14ee8fd4f9ea7f9e7533d_fe4ae974_14fd8b6a\Report.wer	10416	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 36 00 36 00 36 00 31 00 37 00 32 00 35 00 39 00 34 00	MetadataHash=-666172594	success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D5C36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D5C1FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 01 00 00 00 00 00 00 13 03 D3 77 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6D5C1FE8	RegSetValueExW

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

Analysis Process: WerFault.exe PID: 1372, Parent PID: 964

General

Target ID:	12
Start time:	12:35:17
Start date:	03/11/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 964 -s 844
Imagebase:	0xb50000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
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	6D5B1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D5A497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C46.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C46.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_69aa54bf4562ff7e548e4d05abc368941456d4_82810a17_050990c9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_69aa54bf4562ff7e548e4d05abc368941456d4_82810a17_050990c9\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D5A497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C46.tmp	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C46.tmp.xml	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C75.tmp.csv	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8D9F.tmp.txt	success or wait	1	6D5A497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 76 fd 63 63 fd 05 12 00 00 00 00 00	MDMP vcc	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	8092	6	00 00 00 00 00 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1f 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 03 00 00 6d fd 63 63 00 00 00 00 00 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 31 00 00 00 00 00 00 00 01 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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	UBGenuineIntelWTmcc01W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	9626	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 fd 7f fd 00 fd 7e fd 00 03 00 00 00 fd 7f fd 00 fd fd fd 00 13 03 fd 77 23 00 00 00 fd 02 00 00 fd fd fd 00 2b 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 fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++~w#+	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	1632	168	74 17 00 00 00 00 00 00 09 04 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 13 03 fd 77 00 00 00 00 01 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 02 00 00 fd 25 00 00	tw%	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	13206	20	17 00 00 00 fd 02 fd 77 00 00 00 00 00 01 00 00 0a 35 00 00	w5	success or wait	23	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	13578	256	fd 77 05 0f fd 2f 5f 05 00 fd 45 fd 24 00 00 00 fd 45 fd 01 00 00 00 6a 07 59 33 fd fd 7d fd fd 53 fd 4d fd fd fd 00 00 fd 75 fd 66 39 73 fd 75 33 fd 45 fd 01 00 00 00 56 56 fd 53 0b 4d fd fd 25 fd 00 00 fd 75 fd fd 45 fd fd fd fd fd 1c 00 00 00 fd 45 fd 00 fd 43 fd fd fd fd fd 04 00 cd 53 fd 33 fd fd 2b 09 00 00 fd fd fd 4d fd fd 1d 01 00 fd 6a 03 59 fd 29 fd fd 55 fd fd fd 24 fd 58 fd fd 77 53 56 57 fd fd fd 03 fd 0f 6b fd 5c 6a 40 fd 4d fd fd fd 48 7c fd 77 40 fd 58 fd fd 77 fd 47 18 fd fd 40 7c fd 77 fd 47 20 fd fd 44 7c fd 77 0f fd 5f 2c 58 66 3b fd 0f fd 69 01 00 00 0f fd fd 50 fd 77 30 fd 45 fd fd fd 54 7c fd 77 50 fd 6a fd 03 00 fd 4d fd fd fd 0c fd fd 4d fd 6a 40 58 66 3b fd 73 10 6b 45 fd 2e 03 fd 33 fd 66	w/_E$EjY3}SMuf9su3EVVSM%uEECS3+MjY)U$XwSVWk\j@MH|w@XwG@|wG D|w_,Xf;iPw0ET|wPjMMj@Xf;skE.3f	success or wait	22	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	41266	256	fd 0c 00 fd fd 08 10 00 00 fd 10 78 fd 76 fd fd fd 04 00 fd fd 09 10 00 00 fd 10 78 fd 76 fd fd fd 10 00 fd fd 0a 10 00 00 fd 10 78 fd 76 fd fd fd 1c 00 fd fd 0b 10 00 00 fd 10 78 fd 76 fd fd fd 2c 00 fd fd 0c 10 03 00 fd 10 78 fd 76 fd fd fd 04 00 fd fd 0d 10 03 00 fd 10 78 fd 76 fd fd fd 04 00 fd fd 0e 10 07 00 fd 10 78 fd 76 fd fd fd 08 00 fd fd 0f 10 01 00 fd 10 78 fd 76 fd fd cd 49 00 fd 10 10 00 00 fd 10 78 fd 76 fd fd fd 08 00 fd fd 11 10 00 00 fd 10 78 fd 76 fd fd fd 08 00 fd fd 12 10 00 00 fd 10 78 fd 76 fd fd fd 10 00 fd fd 13 10 07 00 fd 10 78 fd 76 fd fd fd 08 00 fd fd 14 10 00 00 fd 10 78 fd 76 fd fd fd 0c 00 fd fd 15 10 01 00 fd 10 78 fd 76 fd fd cd 49 00 fd 16 10 14 00 fd 10 78 fd 76 fd fd fd 10 00 fd fd 17 10 00 00 fd 10 78 fd 76 fd	xvxvxvxv,xvxvxvxvIxvxvxvxvxvxvIxvxv	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	1800	4	04 00 00 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	10342	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 7f fd 00 fd fd fd 00 13 03 fd 77 23 00 00 00 fd 02 00 00 fd fd fd 00 2b 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 fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w#+	success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	1948	48	24 05 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 3e 00 00 00 00 00 fd fd 04 00 00 00 00 18 10 00 00 7e 4c 00 00 fd 02 00 00 fd 30 00 00	$ ~L0	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	2008	4	32 00 00 00	2	success or wait	50	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	8098	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	50	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	7304	120	00 00 fd 6f 00 00 00 00 00 60 0d 00 20 fd 0d 00 fd 0c fd 5a 25 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 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	o` Z%BB?%@A	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	9592	34	1c 00 00 00 35 00 69 00 69 00 58 00 79 00 4e 00 56 00 43 00 51 00 33 00 2e 00 64 00 6c 00 6c 00 00 00	5iiXyNVCQ3.dll	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	7424	668	00 00 00 10 00 00 00 00 00 fd 0d 00 00 00 00 00 00 00 00 00 78 25 00 00 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 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 20 fd 02 00 00 00 00 00 10 03 03 00 00 00 00 1a 4e 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 77 03 00 00 00 00 00 0a 79 03 00 00 00 00 00 00 00 00 00 00 00 00 fd 4f 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 75 fd 04 00 00 00 00 00 26 4f 5f 7b 00 00 00 00 fd fd fd 17 00 00 00 00 fd 4d 5a 10 00 00 00 00 fd 1b 7e 01 00 00 00 00 7e fd 00 00 fd fd 00 00 fd fd 05 00 59 14 0b 00 fd fd 04 00 06 fd 1f 00 75 fd 04 00 fd fd 24 00 fd 26 01 00 05 fd 0f 00 00 00 00 00 16 37 15 00 fd 6b 04	x%Zb NwyO@u&O_{MZ~~Yu$ &7k	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	41522	12710	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	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER885C.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 1c 15 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 1c 00 00 05 00 00 00 74 01 00 00 fd 33 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 21 00 00 08 fd 00 00 15 00 00 00 fd 01 00 00 18 1d 00 00 16 00 00 00 fd 00 00 00 04 1f 00 00	$t3`8T!	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	964	28	3c 00 50 00 69 00 64 00 3e 00 39 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>964</Pid>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	992	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	996	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1000	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1070	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1074	2	09 00		success or wait	2	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1078	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1168	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1172	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1176	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 37 00 37 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>9770</Uptime>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1218	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1222	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1226	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1430	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 36 00 32 00 34 00 38 00 30 00 31 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>162480128</PeakVirtualSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1518	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1522	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1528	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 36 00 32 00 32 00 35 00 30 00 37 00 35 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>162250752</VirtualSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1610	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 34 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>4464</PageFaultCount>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1694	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 34 00 31 00 37 00 39 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>14417920</PeakWorkingSetSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1802	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 34 00 31 00 37 00 39 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>14417920</WorkingSetSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1884	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1888	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	1894	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 33 00 33 00 34 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>233480</QuotaPeakPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2008	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2012	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2018	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 32 00 38 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>232864</QuotaPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2116	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2120	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2126	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 32 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>48240</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2250	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2254	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2260	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 31 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>48104</QuotaNonPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2368	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2372	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2378	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 32 00 37 00 33 00 39 00 32 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>8273920</PagefileUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2454	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2458	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2464	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 32 00 37 00 38 00 30 00 31 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>8278016</PeakPagefileUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2556	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2560	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2566	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 32 00 37 00 33 00 39 00 32 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>8273920</PrivateUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2638	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2642	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2646	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2692	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2696	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2700	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2730	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2734	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2740	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	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2780	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2784	2	09 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2792	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3144</Pid>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2822	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2826	2	09 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2834	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 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>loaddll32.exe</ImageName>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2906	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2910	2	09 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	2918	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3008	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3012	2	09 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3020	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 31 00 34 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10148</Uptime>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3064	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3068	2	09 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3076	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3158	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3162	2	09 00		success or wait	4	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3170	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3222	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3226	2	09 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3234	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3278	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3282	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3292	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 30 00 33 00 39 00 35 00 33 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>110395392</PeakVirtualSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3380	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3384	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3394	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 30 00 32 00 31 00 34 00 34 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>105021440</VirtualSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3466	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3470	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3480	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 31 00 37 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>3173</PageFaultCount>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3568	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 30 00 34 00 35 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>10604544</PeakWorkingSetSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3666	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3670	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3680	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 30 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>10604544</WorkingSetSize>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3762	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3766	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3776	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 34 00 39 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>249544</QuotaPeakPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3890	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3894	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	3904	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 30 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>239048</QuotaPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4002	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4006	2	09 00		success or wait	5	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4016	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 31 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>40112</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4140	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4144	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4154	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 39 00 39 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>39976</QuotaNonPagedPoolUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4262	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4266	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4276	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 32 00 35 00 31 00 36 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4251648</PagefileUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4352	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4356	2	09 00		success or wait	5	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4366	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 32 00 35 00 35 00 37 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>4255744</PeakPagefileUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4458	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4462	2	09 00		success or wait	5	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4472	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 32 00 35 00 31 00 36 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4251648</PrivateUsage>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4544	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4548	2	09 00		success or wait	4	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4556	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4602	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4606	2	09 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4612	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4654	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4658	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4662	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4694	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4698	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4700	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4742	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4746	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4748	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4786	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4790	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4794	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4846	4	0d 00 0a 00		success or wait	9	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4850	2	09 00		success or wait	18	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	4854	74	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 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</Parameter0>	success or wait	9	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	5538	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	5542	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	5544	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	5584	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	5588	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	5590	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	5628	4	0d 00 0a 00		success or wait	6	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	5632	2	09 00		success or wait	12	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	5636	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6190	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6194	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6196	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6236	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6240	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6242	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	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6288	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6382	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6386	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6390	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 65 00 6a 00 79 00 65 00 73 00 6c 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>ejyesl, Inc.</SystemManufacturer>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6496	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6500	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6504	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 65 00 6a 00 79 00 65 00 73 00 6c 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>ejyesl7,1</SystemProductName>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6600	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6604	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6608	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6728	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6732	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6736	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 32 00 37 00 32 00 38 00 38 00 33 00 35 00 39 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>1627288359</OSInstallDate>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6818	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6822	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6826	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6928	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6932	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	6936	70	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 2d 00 30 00 31 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>-01:00</TimeZoneBias>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7006	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7010	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7012	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7052	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7056	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7058	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7092	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7096	2	09 00		success or wait	2	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7100	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7196	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7200	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7202	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7238	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7242	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7244	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7268	4	0d 00 0a 00		success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7272	2	09 00		success or wait	6	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7276	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>80000000</Flags>	success or wait	3	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7522	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7526	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7528	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7554	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7558	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7560	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 31 00 31 00 2d 00 30 00 33 00 54 00 31 00 31 00 3a 00 33 00 35 00 3a 00 31 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-03T11:35:19Z">	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7660	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7664	2	09 00		success or wait	2	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7668	260	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 32 00 39 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 39 00 36 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 36 00 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 36 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 00 3d 00 22 00 31	<Process AsId="294" PID="964" UptimeMS="6968" TimeSinceCreationMS="6968" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7928	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7932	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7936	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7956	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7960	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	7962	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	8000	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	8004	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	8006	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	8052	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 35 00 63 00 62 00 37 00 31 00 37 00 65 00 2d 00 66 00 37 00 30 00 61 00 2d 00 34 00 37 00 31 00 64 00 2d 00 39 00 30 00 37 00 31 00 2d 00 35 00 34 00 62 00 37 00 65 00 66 00 39 00 36 00 31 00 65 00 36 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>75cb717e-f70a-471d-9071-54b7ef961e65</Guid>	success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	2	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	8158	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 31 00 31 00 2d 00 30 00 33 00 54 00 31 00 31 00 3a 00 33 00 35 00 3a 00 31 00 39 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>2022-11-03T11:35:19Z</CreationTime>	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	8256	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	8260	2	09 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	8262	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	8302	4	0d 00 0a 00		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B4B.tmp.WERInternalMetadata.xml	8306	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	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C46.tmp.xml	0	4731	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 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_69aa54bf4562ff7e548e4d05abc368941456d4_82810a17_050990c9\Report.wer	0	2	fd fd		success or wait	1	6D5A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_69aa54bf4562ff7e548e4d05abc368941456d4_82810a17_050990c9\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	178	6D5A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_69aa54bf4562ff7e548e4d05abc368941456d4_82810a17_050990c9\Report.wer	12062	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 32 00 30 00 35 00 38 00 38 00 31 00 30 00 36 00 38 00 39 00	MetadataHash=-2058810689	success or wait	1	6D5A497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D5A43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6D5C36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6D5C36BF	unknown
\REGISTRY\A\{82319504-c857-892a-1691-677d3695f0d2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6D5C36BF	unknown

Disassembly

No disassembly