ID: 628121
Sample Name: BJp3aUvrt9
Cookbook: default.jbs
Time: 10:59:07
Date: 17/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

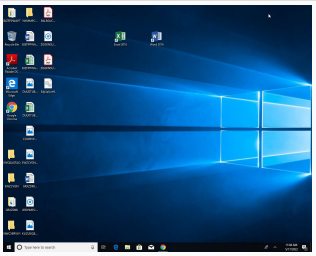
Windows Analysis Report

BJp3aUvrt9

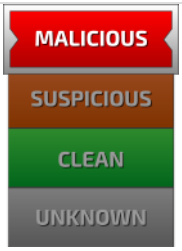
Overview

General Information

Sample Name:	BJp3aUvrt9 (renamed file extension from none to dll)
Analysis ID:	628121
MD5:	9046f78804227b..
SHA1:	37ddabb88b9092.
SHA256:	e34af6effb59651..
Tags:	dll
Infos:	



Detection



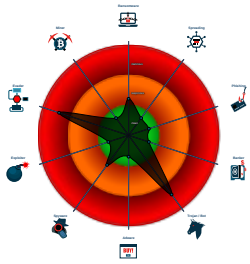
Ursnif

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Found API chain indicative of debug…
- Machine Learning detection for sam…
- Found evasive API chain (may stop…
- Writes registry values via WMI
- Uses 32bit PE files
- One or more processes crash

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6424 cmdline: loaddll32.exe "C:\Users\user\Desktop\BJp3aUvrt9.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6452 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\BJp3aUvrt9.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6472 cmdline: rundll32.exe "C:\Users\user\Desktop\BJp3aUvrt9.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 6532 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6424 -s 388 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6604 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6424 -s 396 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6800 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6424 -s 424 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"uFHdIp1dwWhvkEA2yTiBbeuMW6YDB1lsKD5xr+wbKQpSTgCxKW/AXnU7L/HiYIBOAaOvelJb2/pY2jRw/FTeNeGEktAn4DWXMKOPXXT0NA64cjWTlmZ01c3ZQu3caOM/Vp3zMRoE3uvOCFkw5pB9m5AVXCHf7c66rMBTCpzNlB06TLav
0Zslv7QoNXagpBRObC3w6aRV9zoEMPsKo8dDtjcXrpjT3cmo/nK2BeLeCRHw4m+Z1wNt/QFKG0JSvLN7KWGp2TqLTGCk8sWmJopJGBcCeH8dEEcUduFFgdi8Cilu/K4cd0diqylW1QdRW2VJSAgt/TyNLQ8XGjESLVVFp5dI5rtAU8yov
Xe+vZ9IsF8=",
  "c2_domain": [
    "config.edge.skype.com",
    "185.189.151.28",
    "185.189.151.70"
  ],
  "botnet": "3000",
  "server": "50",
  "serpent_key": "noA8W2qeaw7z6wk9",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000003.364421717.00000000051A8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.364070986.00000000051A8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.364312063.00000000051A8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.364235828.00000000051A8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.364148388.00000000051A8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.rundll32.exe.8f0000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.2.rundll32.exe.10f0000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.2.rundll32.exe.49c94a0.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.2.rundll32.exe.49c94a0.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.3 - Destination IP: 13.107.42.16

Timestamp:	192.168.2.313.107.42.1649754802033203 05/17/22-11:01:06.002753
SID:	2033203
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

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

Copyright Joe Security LLC 2022

Snort IDS alert for network traffic

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

System Summary

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Malware Analysis System Evasion

Found evasive API chain (may stop execution after checking system information)

Anti Debugging

Found API chain indicative of debugger detection

HIPS / PFW / Operating System Protection Evasion

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

Stealing of Sensitive Information

Yara detected Ursnif

Remote Access Functionality

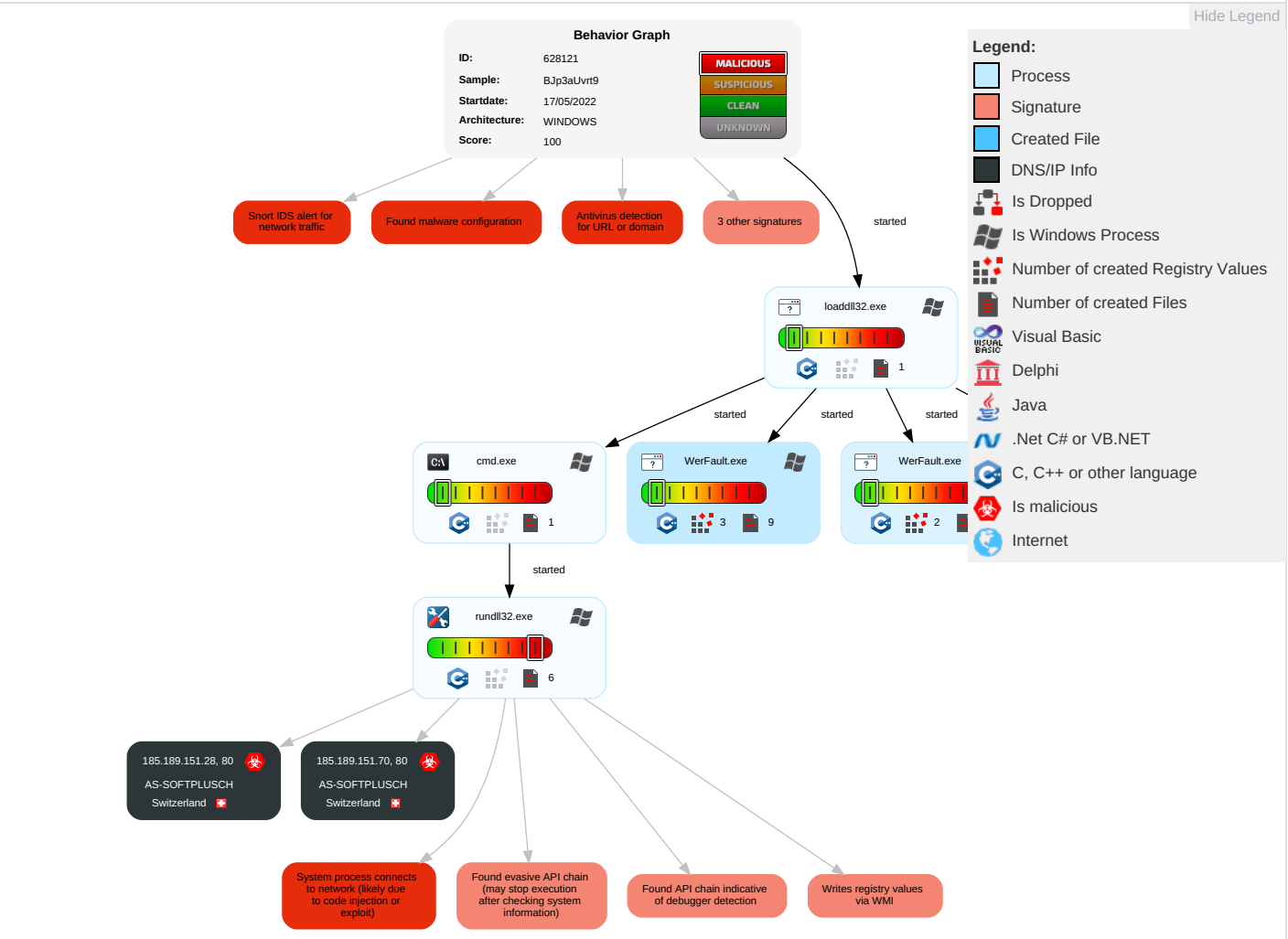
Yara detected Ursnif

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 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	1 2 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 1 Process Injection	LSASS Memory	1 1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	1 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Rundll32	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Account Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Remote System 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 1 4 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

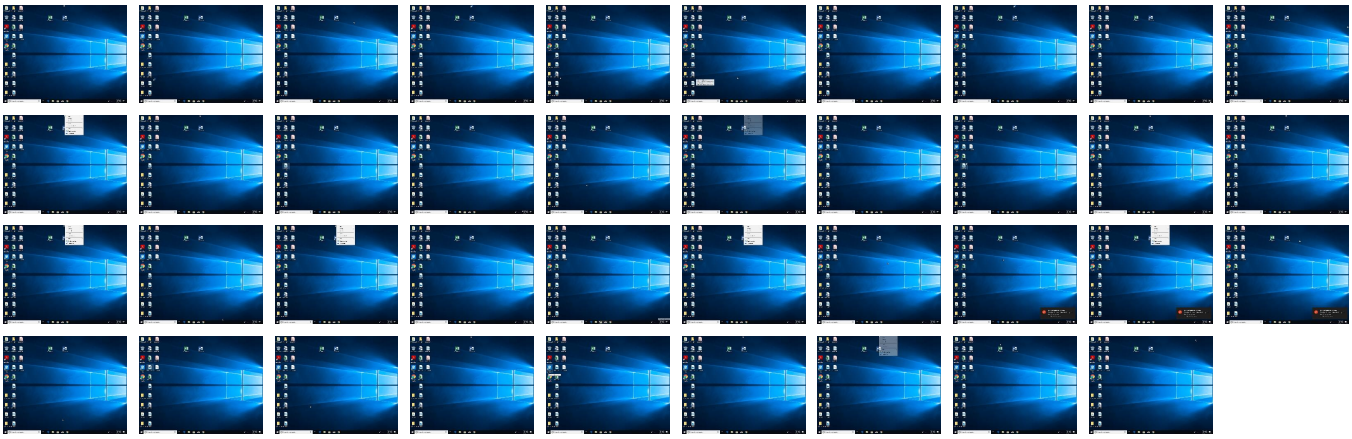
Behavior Graph



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
BJp3aUvrt9.dll	32%	ReversingLabs	Win32.Trojan.Generic	
BJp3aUvrt9.dll	100%	Joe Sandbox ML		

Copyright Joe Security LLC 2022

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.8f0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.rundll32.exe.10f0000.1.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.189.151.28/	100%	Avira URL Cloud	malware	
http://185.189.151.28/drew/Gno4E_2Fz/JYCqWA_2FqMmY1RZwoiB/wugIArNn94bFR0HD9u1/3DvnzuRELDO66MgbIMgnTX	100%	Avira URL Cloud	malware	
http://185.189.151.70/?	100%	Avira URL Cloud	malware	
http://185.189.151.70/	100%	Avira URL Cloud	malware	
http://185.18	0%	Avira URL Cloud	safe	

Domains and IPs

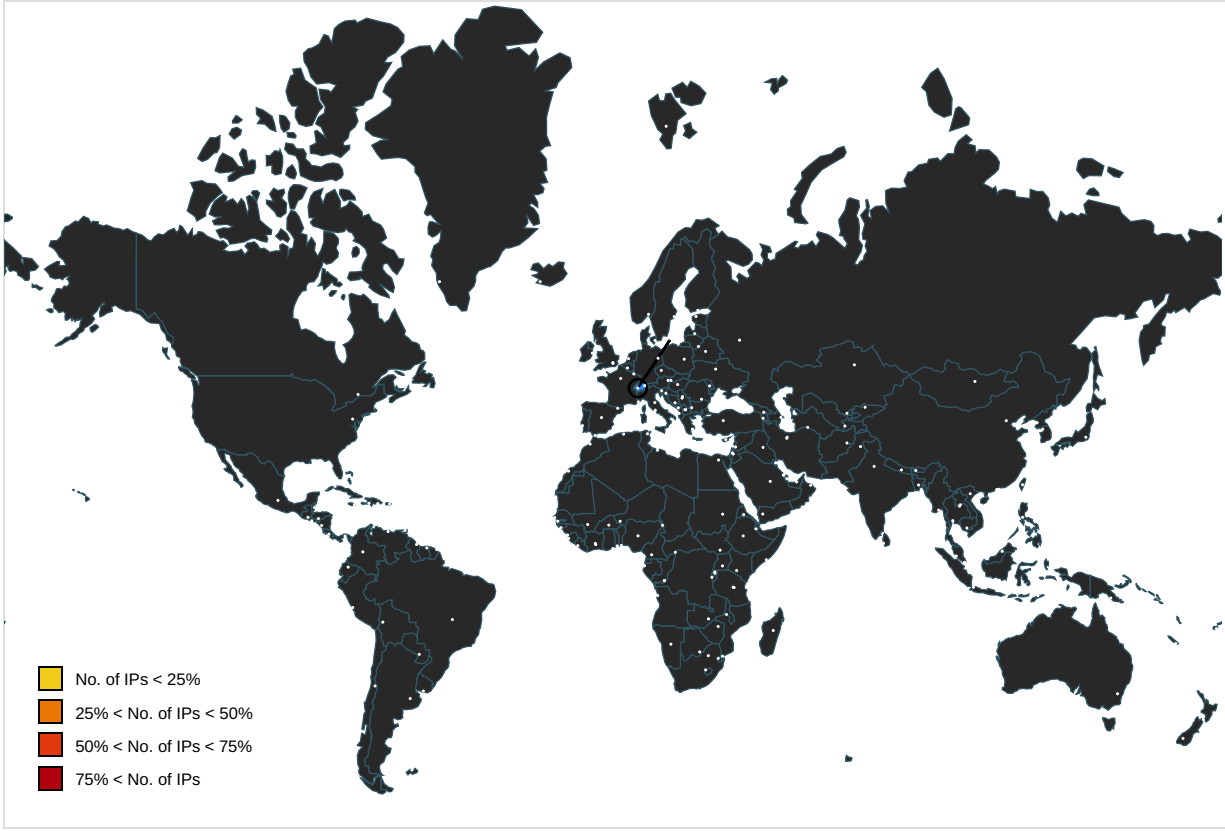
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://185.189.151.28/	rundll32.exe, 00000002.00000002.78473015 0.0000000000A76000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://185.189.151.28/drew/Gno4E_2Fz/JYCqWA_2FqMmY1RZwoiB/wugIArNn94bFR0HD9u1/3DvnzuRELDO66MgbIMgnTX	rundll32.exe, 00000002.00000002.78473015 0.0000000000A76000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://185.189.151.70/?	rundll32.exe, 00000002.00000002.78473015 0.0000000000A76000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://185.189.151.70/	rundll32.exe, 00000002.00000002.78464657 9.0000000000A49000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 002.00000002.784730150.0000000000A76000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://185.18	rundll32.exe, 00000002.00000002.78488223 1.00000000010DC000.00000004.00000010.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.189.151.70	unknown	Switzerland		51395	AS-SOFTPLUSCH	true
185.189.151.28	unknown	Switzerland		51395	AS-SOFTPLUSCH	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	628121
Start date and time: 17/05/202210:59:07	2022-05-17 10:59:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BJp3aUvrt9 (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@8/12@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 45.6% (good quality ratio 42.2%) • Quality average: 79% • Quality standard deviation: 30.7%

Copyright Joe Security LLC 2022

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 52.182.143.212, 13.107.42.16
- Excluded domains from analysis (whitelisted): fs.microsoft.com, config.edge.skype.com.trafficmanager.net, arc.msn.com, ris.api.iris.microsoft.com, onedsblobprdcus15.centralus.cloudapp.azure.com, store-images.s-microsoft.com, login.live.com, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, l-0007.l-msedge.net, config.edge.skype.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:00:28	API Interceptor	2x Sleep call for process: WerFault.exe modified
11:01:00	API Interceptor	1x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_13ec5c98984773435626ad7d5b7558cb4938ccf_7cac0383_1985ef9c\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536

Entropy (8bit):	0.7490316764233721
Encrypted:	false
SSDEEP:	96:gG6uFxLWJnYyCy9haot7JnOpXIQcQac6pcEccw35+a+z+HbHgIVG4rmMXL9iVffk:xbGnaH0tGtjbq/u7skS274ItW
MD5:	24141771F0348D4D2165E1C941A1787B
SHA1:	9547CBA944AE3D174D3CEC21B225C3F54AB002DF
SHA-256:	ABB363145D8BCAFB5E2786F6AEC6B37A633B62DB331E531EFDD265EE6371D88D
SHA-512:	237007822C3FB9D4614D327742330E58707753128FE980A2D24D4FB530461B645E8D4E00B82DC190E762E79820ACA3424B468226728D7DF8B88D5C4CD3221138
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.2.8.4.0.2.4.6.6.5.4.3.0.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.2.8.4.0.2.6.4.1.5.4.0.5.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.3.d.a.8.2.5.c.-.3.6.4.c.-.4.5.d.6.-.b.c.5.3.-.d.9.f.f.4.d.e.7.4.c.e.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.=.8.2.7.5.9.0.3.b.-.2.2.d.6.-.4.b.5.9.-.9.8.1.6.-.6.3.e.f.9.8.2.5.0.9.2.8.....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.=.0.0.0.0.1.9.1.8.-.0.0.0.1.-.0.0.1.d.-.9.e.b.3.-.5.3.f.6.1.7.6.a.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.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_61eae61638761e2a39674020347ca413fb22393_7cac0383_19cdd4c1\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7419357989377661
Encrypted:	false
SSDEEP:	96:UfiBTWJnYypy9haFCj+kSZpXIQcQac6pcEccw35+a+z+HbHgIVG4rmMXL9iVff9o:yiBCnXH0tGtjbq/u7s/S274Itb
MD5:	22BEBF100C00B60C01CD3402F3B3779B
SHA1:	200682AEFFBEA38E807BF478AC5A74612C870AC6
SHA-256:	7BDC06AB615B766001F79167D9C844ABB7463A379739C0FC099B9D176ADD1ABF
SHA-512:	0761F41B6B3210F299F3FB985F3FBCECDDE0EC468A6EF9DD5486541CA0807331254F276C78B4CB134A16DBA030D9CC3CCA9C9CB103FC54DE27F96626EEE3F FA
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.2.8.4.0.1.9.4.9.0.2.8.0.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.4.e.3.4.3.6.7.-.7.3.e.6.-.4.b.7.8.-.8.8.7.3.-.0.f.a.0.4.a.f.3.4.b.f.d.....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.=.f.c.4.8.b.8.d.e.-.8.c.4.f.-.4.4.2.5.-.9.e.b.7.-.6.c.f.9.1.2.b.0.7.0.3.8.....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.=.0.0.0.0.1.9.1.8.-.0.0.0.1.-.0.0.1.d.-.9.e.b.3.-.5.3.f.6.1.7.6.a.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.=.2.0.2.1././.1.2././.1.3.:.0.9.:.0.7.:.1.6.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b75bd23440526356a090f9cb45508f9dce6e86_7cac0383_1ada168d\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7452090624012112
Encrypted:	false
SSDEEP:	96:ctF/k8WJnYymy9haFCjmfIpXIQcQsc6LcENcw3CM+a+z+HbHgIVG4rmMXL9iVffk:kmxnXHSPX7jbq/u7skS274ItW
MD5:	D39E373EA80BDB4ABEA47E895F4CDB01
SHA1:	C175A2016669C7E8C44BDF09002D5BDF1C4F24F7
SHA-256:	BEE31382B92DAFF45275431A897D4A8D0D2028075B05A75555752C54D8C58E74
SHA-512:	601E58D0DA8F7E1051A95F095ED7579C3D72F917EFA0D780A481E89A95280B48582835AB7F7E715A9845AFA8B8FFE71382368CC227C1B7A986A045B0364A33B3
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.2.8.4.0.3.5.2.2.8.5.1.2.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.2.8.4.0.3.6.9.3.1.6.4.4.7.....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.=.7.2.6.4.5.9.b.c.-.f.f.6.b.-.4.1.0.5.-.9.5.4.a.-.f.a.e.9.1.8.d.6.4.9.7.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.9.2.7.7.9.d.c.-.0.b.c.d.-.4.6.f.9.-.b.d.2.a.-.1.c.0.5.6.1.3.4.7.c.4.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.1.9.1.8.-.0.0.0.1.-.0.0.1.d.-.9.e.b.3.-.5.3.f.6.1.7.6.a.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.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1046.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe

File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4558
Entropy (8bit):	4.428766017452063
Encrypted:	false
SSDEEP:	48:cvIwSD8zshJgtWI9kiWgc8sqYjz38fm8M4J2+A+XFqz+q84fSvg2KcQlcQw0hdd:uITfzPjgrsqYPcJ/qMnKkw0hdd
MD5:	AA35D5A5B6894F05AC4C0E9A9332472F
SHA1:	494B810764D38A322B11D47A081871CE22B83BA7
SHA-256:	31F35E36D5DA16819901B80714ACBD7C4EBB1D5910A42472EB79E48AE52E1A83
SHA-512:	040CB17A5E12566F27FCB923158FDCDF70B6ABA1840C3F818D0F1B82E77FFADCE5FDD1981B8F8B34118F40C6C36749DA251A95CF4AF50093E438E0D2A693AE4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1519391" />.. <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\WERB04.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue May 17 18:00:35 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	47674
Entropy (8bit):	2.2871381466825977
Encrypted:	false
SSDEEP:	384:8PezsKaQ+EuwDScxGzTGcwiO3vDL/2B/zp70cU3:8PusWgwDvGXK3vDLu83
MD5:	5509847FFAD6A604DCEE3BDBA5607C73
SHA1:	14EF85682E5123F94333D10002631DF22EA02051
SHA-256:	0D88E25046E05ED8E98E65545C0143D7B942FE251A55E249D25E0A14B8BDFB5B
SHA-512:	911659359456CCF6FE9B17722E9C4D849D7E225B8EEBAF711ECE5C3DBF45AC345A52E0EFF03B3FB35EDD32297F74F119296B0DEA97E67B94B8FDD0E7F2819844
Malicious:	false
Preview:	MDMP..... .....b.....L.....$.....~!.....`.....8.....T.....U.....B..... ..GenuineIntelW.....T.....b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...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\WERCD7E.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue May 17 18:00:19 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	34850
Entropy (8bit):	2.045569064677871
Encrypted:	false
SSDEEP:	192:oFHM+tYEjEOPxMrUwz23RiuqCkI6lKWesjR+6:9yPOlwz2B/rp60Wes
MD5:	DBE2F603F81E822005E12B636CC8F37A
SHA1:	52BF00112ECD0672AA3EAE48C6BBCAB030F8870C
SHA-256:	F1F7B4F8CDCAC7FB076326CCB3F3BBAD1ECF976F0BAB451728053A494BFD036D
SHA-512:	F0D01F7FBCD8C147AFC11A675B64A6CB3C85EE7E116FCD03A5AB4F8587DE635D131B378537CBAFA17A8E829BBDBB38CC665D540E4126264C6A4EBB8DD83B92F6
Malicious:	false
Preview:	MDMP..... .....b.....L.....$.....~!.....`.....8.....T.....rx.....U.....B..... ..GenuineIntelW.....T.....b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...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\WERD06D.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped

Size (bytes):	8346
Entropy (8bit):	3.6893675787544065
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNieA6l06YWySUOuKgmfHSvCpNj89b4p1fTibIm:RrlsNip6l06YjSUOuKgmfHSF4LfTiB
MD5:	4987BD8F38F3176EA061DE3C70FFB3AE
SHA1:	B8E8C8BE9218A26830068FEF0E4D2E9ACAB109C4
SHA-256:	C71E98FB80478A643390D78BDCE471BF2A841F44F5D9DBAD9D7B8325E572E37F
SHA-512:	50675E5D76C5A334E9F37BE06ADF82377517766DF3011162042ED016ED8E55CACC89E54385181FC09D279937186B17FB886D097B13706150465CA03C8D7AB0A7
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.4.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1D5.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):	4.418360328033601
Encrypted:	false
SSDEEP:	48:cvIwSD8zsaJgtWI9kiWgc8sqYj08fm8M4J2+AKkFag+q8vQ+AKB2KcQIcQw0h8d:uITfoPjgrsqYVJPNgKxEKkw0h8d
MD5:	F24A79F2EBB558B3CF4BA99D079908A2
SHA1:	680AE2D2E24E3288847EA0EF881E04912FB10BCA
SHA-256:	226C608C343E7570FA0F48FAAE525A49D5D113FE8D07AF42D78108C8CC7D9215
SHA-512:	C4E38045B7DC09B6210A203FE2899EC5AFA4DCE8C43D9DEA22AB348711F82540175FBEEA6EE487A14C68AF65A2B977B8AB5F821473E6E12ABC1B52CD358C5C05
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="1519390" />.. <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\WERE1F0.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue May 17 18:00:25 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	34650
Entropy (8bit):	1.9851963209158827
Encrypted:	false
SSDEEP:	192:+ws3+xSbOPnFgq6r23RiuiCkIFlKnP+meCxy/YepTB:pSiPnFgq6r2B/jpF0nP++M
MD5:	0277A1753C5E96067D53F043D6A85F77
SHA1:	EB9C9E8B4B62E292C908336CB2107C02465F1B57
SHA-256:	AB2DF3ABD65E75703AD26565148A893AE2A15CE0FD41071BF5151B2969022F51
SHA-512:	1853C2EB35870652AB6F6B561EB85F61B7C53C186FC01B1FD88ED636F03B730C5033C93C8B65323AA24A91E3D3D745EBC87B2014CF3C1D8781AF19A26A6BA6F8
Malicious:	false
Preview:	MDMP..... .....b.....L.....$.....~!.....`.....8.....T.....w.....U.....B..... ..GenuineIntelW.....T.....b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...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\WERE56C.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8334
Entropy (8bit):	3.6989805425570728
Encrypted:	false

SSDEEP:	192:Rrl7r3GLNiejZ6cx6YWuSUMZgmffSvCprj89blBsfPXm:RrlsNiwZ6cx6YfSUMZgmffSzl6fe
MD5:	4FE019ACEA2068A2CD647811D69D21E8
SHA1:	B21371DC73D60C8D53024F300146D13897B5BAE4
SHA-256:	980C155A61157C06A302625AF339D1E5BB2F246C7CBCCB5A29E4F489A1346D05
SHA-512:	183C013E53A9F4D8EA635A5A83804E5D28FB80BD2104993238226D11E349760DBD82DB8BB2B21372665BF4BADB17317008F71B2E679F77A16177C05A287A7B10
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.4.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE732.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4598
Entropy (8bit):	4.471011953494763
Encrypted:	false
SSDEEP:	48:cvIwSD8zshJgtWI9kiWgc8sqYj68fm8M4J2+cZFi+q849BG2KcQIcQw0hdd:uITfzPjgrsqYrJ+W3ZKkw0hdd
MD5:	43BF7F96677B46482AE400E7B338E641
SHA1:	D3EE1BCAE6406790456723BBAEDE3B42E9A39142
SHA-256:	D08290638FE248B9BC31E7D9304B44AD74E160EB2ABE1CC23F60671E97AF332A
SHA-512:	98C761780969B78AF7642786EDCD32C35C0DC47183489EE0C645A3B270D9C33F394CDE8CFB8D39CB56B450FD8BCF3DE93DC64AA02B4E323140121420900027E
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="1519391" />.. <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\WERE8F.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8288
Entropy (8bit):	3.6923793035917205
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNie+b645Y6YWJSUvAgmf0ScCpDv89b/Bsfl1m:RrlsNir6UY6Y4SUvAgmf0SM/6f2
MD5:	480F9648CE7C0B9612874C9BDA749C5E
SHA1:	ACFBE120FDE9FE114F2D7ACEB29184BAD4200903
SHA-256:	06BBC7172866F02D5460C18C3C13BBC32C5103AE31977EF4172596911AA7695A
SHA-512:	E4DB58FD5D018108D4438B4F62E602EB1D3E665E652FF71CB467221E6053107B05BDFFECD920A6E6A6F3A1FD39E110834C3DC5F351D2B6C9AE9DE00D1064D53
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.4.2.4.<./.P.i.d.>.....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.254248896562745
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:	BJp3aUvrt9.dll
File size:	442368
MD5:	9046f78804227bd742d558325fa8f4c0
SHA1:	37ddabb88b909290e1da368f275448a880887482
SHA256:	e34af6effb596517e32ddf82fb283e8b844ec34d373f4e04e93e9916d26c287d
SHA512:	29051fe2ba6908eee8d68af4331bb830d21ce78830f057783b0b0f9d595d6d6f62b402b31495205c13e14a4f74cedb68f20c693ed2717aa8eaf5704975cae475
SSDEEP:	6144:oW1iktBgcV9yjYJrTOkRLookGIw8OaDSOKdPmo6iJTk/DmpFkbakc+abuFGGGGGD:oW44BgcV9yjY1OkEGx/V72/DmSH6/
TLSH:	5294E00965216A6ED9DC273DC9E1D31B1D62B75CD23E70BE3CF43C9F7AE6125820428A
File Content Preview:	MZ.....@.....(.....0...w+!.W....]v.....4.....Y^.....7.....x.....<.....A.....,.....,%.....{.....7.o.....O.....4.....5.....@.....Rich...

File Icon

Icon Hash:	9068eccc64f6e2ad

Static PE Info

General

Entrypoint:	0x4014d0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x3EC34607 [Thu May 15 07:47:19 2003 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	a2b7486f7219709bc441af397fbc35ab

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add ecx, FFFFFFFFh
call 00007F28450A90AAh
pop eax
pop eax
mov dword ptr [0041461Ch], eax
mov edx, dword ptr [00414738h]
sub edx, 00005289h
call edx
mov eax, ebx
mov dword ptr [00414618h], eax
mov eax, esi
mov dword ptr [00414610h], eax
mov dword ptr [00414620h], ebp
mov dword ptr [00414614h], edi
add dword ptr [00414620h], 00000004h
loop 00007F28450A9057h
mov dword ptr [ebp+00h], eax
nop

Instruction
nop
nop
push esp
pop edi
xor dl, dh
cli
inc ebp
lds eax, fword ptr [ecx+34h]
cmpsb
std
xchg dword ptr [ebp-1ED6E020h], edi
stosd
ror al, cl
dec eax
salc
imul edx, dword ptr [edi+61h], 3Fh
or byte ptr [eax], ch
mov al, 87h
dec ch
cli
xchg eax, edi
inc ebp
fdivr qword ptr [edi-20h]
aas
int 45h
fild word ptr [ebx-1BDC28CCh]
add byte ptr [0237275Fh], dl
inc ebx
js 00007F28450A910Eh
enter 53A9h, 5Ch
rol byte ptr [esi], cl
loop 00007F28450A90CCh
mov byte ptr [edi], bl
stc
xchg byte ptr [ebp+423D73FAh], ah
push 00000074h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdd7c	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x62000	0x9f28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6c000	0xf40	.reloc
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	0xd000	0xb8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb8a0	0xc000	False	0.081298828125	data	1.12180017202	IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_LNK_OVER, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_GPREL, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x121f	0x2000	False	0.18701171875	data	4.11729761685	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_LNK_INFO, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_MEM_READ
.data	0xf000	0x7ac0	0x6000	False	0.376546223958	data	6.0108388439	IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_GPREL, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_MEM_READ
.crt	0x17000	0x1dcbd	0x1e000	False	0.988419596354	data	7.98105173778	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.erloc	0x35000	0x2ca3b	0x2d000	False	0.988259548611	data	7.98162384749	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x9f28	0xa000	False	0.602783203125	data	6.51663069246	IMAGE_SCN_LNK_REMOVE, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_LNK_INFO, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_MEM_READ
.reloc	0x6c000	0x1360	0x2000	False	0.223266601562	data	3.77920644751	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_LNK_INFO, IMAGE_SCN_LNK_OVER, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_GPREL, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x62360	0x666	data	English	United States
RT_ICON	0x629c8	0x485d	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x67228	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 331218944, next used block 4106092544	English	United States
RT_ICON	0x697d0	0xea8	data	English	United States
RT_ICON	0x6a678	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x6af20	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x6b488	0xb4	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x6b540	0x120	data	English	United States
RT_DIALOG	0x6b660	0x158	data	English	United States
RT_DIALOG	0x6b7b8	0x202	data	English	United States
RT_DIALOG	0x6b9c0	0xf8	data	English	United States
RT_DIALOG	0x6bab8	0xa0	data	English	United States
RT_DIALOG	0x6bb58	0xee	data	English	United States
RT_GROUP_ICON	0x6bc48	0x4c	data	English	United States
RT_VERSION	0x6bc98	0x290	MS Windows COFF PA-RISC object file	English	United States

Imports

DLL	Import
USER32.dll	IsWindow, LockWorkStation, ExitWindowsEx, LoadCursorFromFileA, IsWindowEnabled, GetMessagePos, GetClassNameA, GetClientRect, GetUpdateRgn, GetWindowWord
KERNEL32.dll	GlobalFree, GetCommState, LockFile, EnumResourceTypesA, GetProcAddress, GetVolumePathNamesForVolumeNameW, GetShortPathNameW, GlobalMemoryStatus, WriteProcessMemory, GlobalFlags, GetFileTime, GetThreadLocale, LocalHandle, GetBinaryTypeA, GetModuleFileNameA
OLEAUT32.dll	LoadTypeLibEx
msvcrt.dll	strcoll, strftime, strtod, strncmp, fgetwc
GDI32.dll	GetCharWidthFloatA, GetTextMetricsW, GdiFlush, ExtEscape
ADVAPI32.dll	RegGetValueA, EnumServicesStatusExW, FreeEncryptionCertificateHashList, GetUserNameW, GetSidSubAuthorityCount

Version Infos

Description	Data
LegalCopyright	A Company. All rights reserved.
InternalName	
FileVersion	1.0.0.0
CompanyName	A Company
ProductName	
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	myfile.exe
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.313.107.42.164 9754802033203 05/17/22-11:01:06.002753	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49754	80	192.168.2.3	13.107.42.16

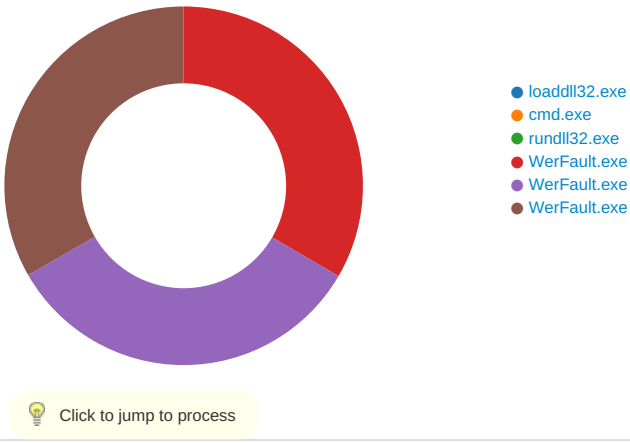
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 17, 2022 11:01:26.059310913 CEST	49755	80	192.168.2.3	185.189.151.28
May 17, 2022 11:01:29.072530031 CEST	49755	80	192.168.2.3	185.189.151.28
May 17, 2022 11:01:35.088505030 CEST	49755	80	192.168.2.3	185.189.151.28
May 17, 2022 11:03:07.316875935 CEST	49825	80	192.168.2.3	185.189.151.70

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 17, 2022 11:03:10.331608057 CEST	49825	80	192.168.2.3	185.189.151.70
May 17, 2022 11:03:16.332169056 CEST	49825	80	192.168.2.3	185.189.151.70

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6424, Parent PID: 5732

General

Target ID:	0
Start time:	11:00:15
Start date:	17/05/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\BJp3aUvrt9.dll"
Imagebase:	0x220000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
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: cmd.exe PID: 6452, Parent PID: 6424

General

Target ID:	1
Start time:	11:00:16
Start date:	17/05/2022

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\BJp3aUvrt9.dll",#1
Imagebase:	0xc20000
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: 6472, Parent PID: 6452

General

Target ID:	2
Start time:	11:00:16
Start date:	17/05/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\BJp3aUvrt9.dll",#1
Imagebase:	0x11d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.364421717.00000000051A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.364070986.00000000051A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.364312063.00000000051A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.364235828.00000000051A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.364148388.00000000051A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.364394991.00000000051A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.364278031.00000000051A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.364350159.00000000051A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000002.785582568.00000000051A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.785174567.00000000049C9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 6532, Parent PID: 6424

General

Target ID:	4
Start time:	11:00:18
Start date:	17/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6424 -s 388
Imagebase:	0xc70000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDF1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1D5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1D5.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_61eae61638761e2a39674020347ca413fb22393_7cac0383_19cdd4c1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_61eae61638761e2a39674020347ca413fb22393_7cac0383_19cdd4c1\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1D5.tmp	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1D5.tmp.xml	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC53.tmp.csv	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC73.tmp.txt	success or wait	1	6DDE497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	5020	6	00 00 00 00 00 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.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 13 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 18 19 00 00 fd fd 62 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 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTb0Pacific Standard TimePacific Daylight Time	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	5710	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 fd 14 fd 00 48 fd 5d 00 00 00 00 00 fd 14 fd 00 fd fd fd fd 20 00 00 00 34 fd 5d 00 fd 14 fd 00 23 00 00 00 02 02 01 00 08 00 5e 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 fd	+S++H] 4]#^+	success or wait	1	6DDE497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	1632	168	1c 19 00 00 00 00 00 00 09 04 00 fd 08 00 00 00 18 fd 5d 00 00 00 00 00 fd 14 fd 00 00 00 00 00 01 00 00 00 00 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 4e 16 00 00	]N	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	8574	20	0e 00 00 00 14 fd 5d 00 00 00 00 00 fd 0c 00 00 62 22 00 00	]b"	success or wait	14	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	8802	3308	fd fd 4c 77 fd 1d 51 77 fd fd fd fd 48 fd 5d 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 34 fd 5d 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 fd 01 00 00 fd fd 5d 00 fd fd fd fd fd 5d 00 12 12 51 77 fd 01 00 00 00 00 00 00 fd fd fd fd 68 fd 5d 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 3c fd 4c 77 00 00 00 00 fd fd fd fd 68 fd 5d 00 18 fd 5d 00 fd 01 00 00 00 00 4d 02 04 00 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 00 00 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd fd fd fd 68 fd 5d 00 fd fd fd fd fd fd 5d 00 fd 17 4d 77 fd fd fd fd 00 00 00 00 fd fd 5d 00 fd 0c 51 77 fd fd fd fd 00 00 00 00 18 fd 5d 00 00 00 00 00 00 00 00 00 70 fd 5d 00 0a 53 77 18 fd 5d 00 68 fd 5d 00 fd fd fd fd 68 fd 5d	LwQwH]4]]]Qwh]<Lwh]]Mh]]Mw]Qw]p]Sw]h]h]	success or wait	13	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	27490	1104	fd fd 4c 77 fd fd 4a 77 fd 00 00 00 fd fd fd fd 10 00 00 00 44 fd fd 00 10 fd fd 00 fd fd fd fd 40 fd 4a 77 40 fd 4a 77 fd fd fd fd 00 fd 67 00 00 fd 67 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd 67 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 30 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 00 fd fd fd fd 00 00 00 00 00 00 00 fd fd fd fd 04 fd 00 00 00 00 00 00 00 00 00 fd 7f fd 00 00 fd 67 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 60 fd fd 00 54 fd 67 00 68 fd fd 00 60 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	LwJwD@Jw@Jwggg0g`Tgh`	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	6426	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 fd fd fd fd 00 00 00 00 00 00 00 00 fd 14 fd 00 fd fd fd 00 00 00 00 58 fd 5d 00 fd fd 4c 77 23 00 00 00 06 02 00 00 18 fd 5d 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	?+S++X]Lw#]+	success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	1900	48	40 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 10 68 00 00 00 00 00 fd fd fd 00 00 00 00 00 6c 04 00 00 4e 2f 00 00 fd 02 00 00 fd 1e 00 00	@ hlN/	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	1960	4	16 00 00 00		success or wait	22	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	5026	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	22	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	4232	120	00 00 fd 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 14 16 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 0c 00 00 00 18 00 00 00 01 00 00 00	t`A!-aBB?#@A	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	5676	34	1c 00 00 00 42 00 4a 00 70 00 33 00 61 00 55 00 76 00 72 00 74 00 39 00 2e 00 64 00 6c 00 6c 00 00 00	BJp3aUvrt9.dll	success or wait	1	6DDE497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	4352	668	00 00 fd 00 00 00 00 00 00 fd 06 00 35 fd 07 00 07 46 fd 3e 2c 16 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 04 00 00 00 00 00 fd 02 00 00 00 00 00 10 0c 03 00 00 00 00 43 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 0d fd 03 00 00 00 00 00 51 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 33 1b 00 00 00 00 00 7d fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 05 00 00 00 00 00 50 fd fd 45 00 00 00 00 29 13 19 00 00 00 00 fd 0f 1b 20 00 00 00 00 fd 72 fd 00 00 00 00 00 7a fd 00 00 fd 0a 01 00 fd fd 05 00 1f fd 0a 00 7d fd 04 00 00 06 7f 15 00 fd 05 00 46 fd 27 00 eb 01 00 e7 11 00 00 00 00 00 fd fd 16 00 6c 5d 04	5F>,ZbCQ3}@PE) rz}F'l]	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	28594	6256	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 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	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7E.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 4c 09 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 10 00 00 05 00 00 00 fd 00 00 00 7e 21 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 0f 00 00 72 78 00 00 15 00 00 00 fd 01 00 00 18 11 00 00 16 00 00 00 fd 00 00 00 04 13 00 00	L$~!`8Trx	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6424</Pid>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1180	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 35 00 35 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4550</Uptime>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1434	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 39 00 37 00 37 00 36 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>52977664</PeakVirtualSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1530	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 30 00 31 00 39 00 32 00 30 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>52019200</VirtualSize>	success or wait	1	6DDE497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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 31 00 36 00 31 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1614</PageFaultCount>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1694	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 39 00 37 00 31 00 39 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>5971968</PeakWorkingSetSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1800	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 39 00 37 00 31 00 39 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>5971968</WorkingSetSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	1890	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 30 00 35 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>100552</QuotaPeakPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2014	96	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 39 00 38 00 35 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>98552</QuotaPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2110	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2114	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2120	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>15744</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2244	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2248	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2254	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 33 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>15392</QuotaNonPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2362	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2366	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2372	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 31 00 34 00 39 00 39 00 31 00 33 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>1499136</PagefileUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2448	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2452	2	09 00		success or wait	3	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2458	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 31 00 35 00 30 00 37 00 33 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>15107328</PeakPagefileUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2550	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2554	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2560	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 31 00 34 00 39 00 39 00 31 00 33 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>1499136</PrivateUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2632	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2636	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2640	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2686	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2690	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2694	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2724	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2728	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2734	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2774	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2778	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2786	30	3c 00 50 00 69 00 64 00 3e 00 33 00 39 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3968</Pid>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2816	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2820	2	09 00		success or wait	4	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2828	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2898	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2902	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	2910	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 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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3000	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3004	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3012	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 38 00 33 00 37 00 30 00 36 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4837067</Uptime>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3072	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3150	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3154	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3162	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3214	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3218	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3226	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	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3270	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3274	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3284	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3388	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3462	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3466	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3476	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 34 00 34 00 34 00 30 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>44403</PageFaultCount>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3552	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3556	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3566	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 33 00 33 00 35 00 30 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>101335040</PeakWorkingSetSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3666	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3670	2	09 00		success or wait	5	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3680	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 30 00 39 00 39 00 30 00 39 00 37 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>100990976</WorkingSetSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3778	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 37 00 39 00 32 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>979216</QuotaPeakPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	3906	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 39 00 32 00 34 00 39 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 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>924912</QuotaPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4018	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 31 00 39 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>70192</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4156	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 38 00 32 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>68288</QuotaNonPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4278	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 39 00 38 00 33 00 39 00 33 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>34983936</PagefileUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4370	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 38 00 36 00 30 00 34 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35860480</PeakPagefileUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4478	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 39 00 38 00 33 00 39 00 33 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>34983936</PrivateUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4564	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4620	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4670	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4708	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4756	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4802	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	9	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	18	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	4862	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	5538	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	5542	2	09 00		success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	5584	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	5588	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	5628	4	0d 00 0a 00		success or wait	6	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	5632	2	09 00		success or wait	12	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6190	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6194	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6236	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6240	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6382	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6386	2	09 00		success or wait	2	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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 76 00 67 00 67 00 6c 00 74 00 77 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>vggltw, Inc.</SystemManufacturer>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6496	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6500	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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 76 00 67 00 67 00 6c 00 74 00 77 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>vggltw7,1</SystemProductName>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6600	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6604	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6728	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6732	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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 31 00 30 00 31 00 34 00 38 00 31 00 33 00 36 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>1610148136</OSInstallDate>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6818	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6822	2	09 00		success or wait	2	6DDE497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6928	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6932	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	6936	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7004	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7008	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7010	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7050	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7054	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7056	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7090	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7094	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7098	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7194	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7198	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7200	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	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7236	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7240	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7242	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7266	4	0d 00 0a 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7270	2	09 00		success or wait	6	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7274	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000F</Flags>	success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7520	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7524	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7526	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7552	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7556	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7558	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 31 00 37 00 54 00 31 00 38 00 3a 00 30 00 30 00 3a 00 32 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-17T18:00:20Z">	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7658	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7662	2	09 00		success or wait	2	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7666	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 33 00 39 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 34 00 32 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 33 00 34 00 38 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 34 00 38 00 34 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="397" PID="6424" UptimeMS="3484" TimeSinceCreationMS="3484" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7928	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7932	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7956	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	7960	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	8000	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	8004	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	8052	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 34 00 65 00 33 00 34 00 33 00 36 00 37 00 2d 00 37 00 33 00 65 00 36 00 2d 00 34 00 62 00 37 00 38 00 2d 00 38 00 38 00 37 00 33 00 2d 00 30 00 66 00 61 00 30 00 34 00 61 00 66 00 33 00 34 00 62 00 66 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>b4e34367-73e6-4b78-8873-0fa04af34bfd</Guid>	success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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 30 00 35 00 2d 00 31 00 37 00 54 00 31 00 38 00 3a 00 30 00 30 00 3a 00 32 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-17T18:00 :20Z</CreationTime>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	8256	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	8260	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.tmp.WERInternalMetadata.xml	8302	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD06D.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1D5.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 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_61eae61638761e2a39674020347ca413fb22393_7cac0383_19cdd4c1\Report.wer	0	2	fd fd		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_61eae61638761e2a39674020347ca413fb22393_7cac0383_19cdd4c1\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	146	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_61eae61638761e2a39674020347ca413fb22393_7cac0383_19cdd4c1\Report.wer	8976	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 32 00 30 00 35 00 30 00 31 00 35 00 34 00 36 00 30 00	MetadataHash=-205015460	success or wait	1	6DDE497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{bb41b84d-43e9-af44-de3f-0e1e3c9875a3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DE036BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6DE01FB2	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 08 00 00 00 18 F5 5D 00 EE 14 85 00 01 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6DE01FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **6604**, Parent PID: **6424**

General

Target ID:	6
Start time:	11:00:23
Start date:	17/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6424 -s 396
Imagebase:	0xc70000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDF1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown

Copyright Joe Security LLC 2022

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE732.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE732.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_13ec5c989847734356 26ad7d5b7558cb4938ccf_7cac0383_1985ef9c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_13ec5c989847734356 26ad7d5b7558cb4938ccf_7cac0383_1985ef9c\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE732.tmp	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE732.tmp.xml	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B.tmp.csv	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3C.tmp.txt	success or wait	1	6DDE497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	5020	6	00 00 00 00 00 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.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 13 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 18 19 00 00 fd fd 62 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 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTb0Pacific Standard TimePacific Daylight Time	success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	5710	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 fd 14 fd 00 48 fd 5d 00 00 00 00 00 fd 14 fd 00 fd fd fd fd 20 00 00 00 34 fd 5d 00 fd 14 fd 00 23 00 00 00 02 02 01 00 08 00 5e 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++H] 4]#^+	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	1632	168	1c 19 00 00 00 00 00 00 fd 01 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 4e 16 00 00	N	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	8574	20	0d 00 00 00 fd fd 5d 00 00 00 00 00 34 0d 00 00 52 22 00 00	]4R"	success or wait	13	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	8786	3380	fd fd 4c 77 fd 1d 51 77 fd fd fd fd 00 fd 5d 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 34 fd 5d 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 fd 01 00 00 fd fd 5d 00 fd fd fd fd fd fd 5d 00 12 12 51 77 fd 01 00 00 00 00 00 00 fd fd fd fd 68 fd 5d 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd 5d 00 07 1e 51 77 00 00 00 00 fd fd fd fd 68 fd 5d 00 10 fd 5d 00 fd 01 00 00 00 00 4d 02 04 00 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 00 00 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd fd fd fd 20 fd 5d 00 fd fd fd fd fd fd 5d 00 fd 17 4d 77 fd fd fd fd 00 00 00 00 fd fd 5d 00 fd 0c 51 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6c fd 5d 00 fd fd 4f 77 10 fd 5d 00 68 fd 5d 00 00 00 00 00 68 fd 5d	LwQw]4]]]Qwh]]Qwh]]M]]Mw]Qwl]Ow]h]h]	success or wait	12	6DDE497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	27290	1104	fd fd 4c 77 fd fd 4a 77 fd 00 00 00 fd fd fd fd 10 00 00 00 44 fd fd 00 10 fd fd 00 fd fd fd fd 40 fd 4a 77 40 fd 4a 77 fd fd fd fd 00 fd 67 00 00 fd 67 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd 67 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 30 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 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 04 fd 00 00 00 00 00 00 00 00 00 fd 7f fd 00 00 fd 67 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 60 fd fd 00 54 fd 67 00 68 fd fd 00 60 fd fd 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	LwJwD@Jw@Jwggg0g`Tgh`	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	6426	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 fd fd fd fd 00 00 00 00 00 00 00 00 fd 14 fd 00 fd fd fd fd 00 00 00 00 10 fd 5d 00 fd fd 4c 77 23 00 00 00 12 02 00 00 fd fd 5d 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	?+S++]Lw#]+	success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	1900	48	40 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 10 68 00 00 00 00 00 fd fd fd 00 00 00 00 00 6c 04 00 00 fd 2f 00 00 fd 02 00 00 fd 1e 00 00	@ hl/	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	1960	4	16 00 00 00		success or wait	22	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	5026	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	22	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	4232	120	00 00 fd 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 14 16 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 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	t`A!-aBB?#@A	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	5676	34	1c 00 00 00 42 00 4a 00 70 00 33 00 61 00 55 00 76 00 72 00 74 00 39 00 2e 00 64 00 6c 00 6c 00 00 00	BJp3aUvrt9.dll	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	4352	668	00 00 fd 00 00 00 00 00 00 fd 06 00 35 fd 07 00 07 46 fd 3e 2c 16 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 04 00 00 00 00 3d 02 00 00 00 00 00 10 0c 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 4e fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2a 1b 00 00 00 00 00 54 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 05 00 00 00 00 00 7a 50 fd 45 00 00 00 00 20 1a fd 19 00 00 00 00 7b 7c 51 20 00 00 00 00 18 fd 07 01 00 00 00 00 fd fd 00 00 5a 1f 01 00 26 22 06 00 fd fd 0a 00 54 fd 04 00 06 7f 15 00 fd 05 00 fd fd 2d 00 fd fd 01 00 fd 20 13 00 00 00 00 00 fd 6c 1b 00 1d 5f 04	5F>,ZbN*T@zPE {|Q Z&"T- l_	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	28394	6256	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 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	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1F0.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 4c 09 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 10 00 00 05 00 00 00 fd 00 00 00 7e 21 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 0f 00 00 fd 77 00 00 15 00 00 00 fd 01 00 00 18 11 00 00 16 00 00 00 fd 00 00 00 04 13 00 00	L$~!`8Tw	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6424</Pid>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.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 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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1180	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 30 00 32 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10022</Uptime>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1232	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1322	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1382	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1436	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 39 00 37 00 37 00 36 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>52977664</PeakVirtualSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1532	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 30 00 31 00 39 00 32 00 30 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>52019200</VirtualSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1612	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 31 00 36 00 34 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1649</PageFaultCount>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 39 00 39 00 32 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>5992448</PeakWorkingSetSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 39 00 38 00 30 00 31 00 36 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>5980160</WorkingSetSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 30 00 35 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>100552</QuotaPeakPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2016	96	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 39 00 38 00 35 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>98552</QuotaPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 31 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>18144</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>17792</QuotaNonPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2374	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 31 00 34 00 39 00 39 00 31 00 33 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>1499136</PagefileUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2460	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 31 00 35 00 30 00 37 00 33 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1507328</PeakPagefileUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2562	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 31 00 34 00 39 00 39 00 31 00 33 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>1499136</PrivateUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2642	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2696	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2736	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	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 39 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3968</Pid>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2830	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	2912	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 38 00 34 00 32 00 35 00 33 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4842539</Uptime>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3074	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3164	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3228	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3286	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3390	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3478	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 34 00 34 00 37 00 31 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>44717</PageFaultCount>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 33 00 33 00 35 00 30 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>101335040</PeakWorkingSetSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3682	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 35 00 37 00 37 00 32 00 36 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>95772672</WorkingSetSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3778	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 37 00 39 00 32 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>979216</QuotaPeakPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	3906	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 39 00 32 00 34 00 39 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 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>924912</QuotaPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4018	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 31 00 39 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>70192</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4156	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 38 00 34 00 32 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>68424</QuotaNonPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4278	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 38 00 33 00 31 00 31 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>29831168</PagefileUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4370	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 38 00 36 00 30 00 34 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35860480</PeakPagefileUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4478	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 38 00 33 00 31 00 31 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>29831168</PrivateUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4564	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4620	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4670	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4708	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4756	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6DDE497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4802	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4864	4	0d 00 0a 00		success or wait	8	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4868	2	09 00		success or wait	16	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	4872	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	8	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	5514	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	5518	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	5520	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	5560	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	5564	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	5566	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	5604	4	0d 00 0a 00		success or wait	6	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	5608	2	09 00		success or wait	12	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	5612	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6166	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6170	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6172	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6212	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6216	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6218	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6256	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6260	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6264	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6358	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6362	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6366	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 76 00 67 00 67 00 6c 00 74 00 77 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>vggltw, Inc.</SystemManufacturer>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6472	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6476	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6480	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 76 00 67 00 67 00 6c 00 74 00 77 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>vggltw7,1</SystemProductName>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6576	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6580	2	09 00		success or wait	2	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6584	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6704	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6708	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6712	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 30 00 31 00 34 00 38 00 31 00 33 00 36 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>1610148136</OSInstallDate>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6794	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6798	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6802	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6912	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6980	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6984	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	6986	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7026	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7030	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7032	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7066	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7070	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7074	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7176	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7212	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7216	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7218	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7242	4	0d 00 0a 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7246	2	09 00		success or wait	6	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7250	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7508	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7512	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7514	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7540	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7544	2	09 00		success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7546	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 31 00 37 00 54 00 31 00 38 00 3a 00 30 00 30 00 3a 00 32 00 35 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-17T18:00:25Z">	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7646	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7650	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7654	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 33 00 39 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 34 00 32 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 30 00 33 00 31 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 30 00 33 00 31 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="397" PID="6424" UptimeMS="6031" TimeSinceCreationMS="6031" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7916	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7920	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7924	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7950	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7988	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7992	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	7994	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	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	8032	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	8036	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	8040	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 33 00 64 00 61 00 38 00 32 00 35 00 63 00 2d 00 33 00 36 00 34 00 63 00 2d 00 34 00 35 00 64 00 36 00 2d 00 62 00 63 00 35 00 33 00 2d 00 64 00 39 00 66 00 66 00 34 00 64 00 65 00 37 00 34 00 63 00 65 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>03da825c-364c-45d6-bc53-d9ff4de74ce5</Guid>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	8138	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	8142	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	8146	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 31 00 37 00 54 00 31 00 38 00 3a 00 30 00 30 00 3a 00 32 00 35 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>2022-05-17T18:00:25Z</CreationTime>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	8244	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	8248	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	8250	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	8290	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE56C.tmp.WERInternalMetadata.xml	8294	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	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE732.tmp.xml	0	4598	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_13ec5c98984773435626ad7d5b7558cb4938ccf_7cac0383_1985ef9c\Report.wer	0	2	fd fd		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_13ec5c98984773435626ad7d5b7558cb4938ccf_7cac0383_1985ef9c\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	147	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_13ec5c98984773435626ad7d5b7558cb4938ccf_7cac0383_1985ef9c\Report.wer	9060	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 39 00 34 00 37 00 37 00 38 00 32 00 38 00 34 00 31 00	MetadataHash=-947782841	success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{7147018a-8ee3-e896-a568-68ca107f99b3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DE036BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 08 00 00 00 18 F5 5D 00 EE 14 85 00 01 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	A5 01 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00	success or wait	1	6DE01FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **6800**, Parent PID: **6424**

General

Target ID:	9
Start time:	11:00:34
Start date:	17/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6424 -s 424
Imagebase:	0xc70000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDF1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1046.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1046.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b75bd23440526356a090f9cb45508f9dce6e86_7cac0383_1ada168d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b75bd23440526356a090f9cb45508f9dce6e86_7cac0383_1ada168d\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDE497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1046.tmp	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1046.tmp.xml	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2931.tmp.csv	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2951.tmp.txt	success or wait	1	6DDE497A	unknown

Copyright Joe Security LLC 2022

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	5020	6	00 00 00 00 00 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.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 13 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 18 19 00 00 fd fd 62 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 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTb0Pacific Standard TimePacific Daylight Time	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	5710	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 fd 14 fd 00 48 fd 5d 00 00 00 00 00 fd 14 fd 00 fd fd fd 20 00 00 00 34 fd 5d 00 fd 14 fd 00 23 00 00 00 02 02 01 00 08 00 5e 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 fd	?+S++H] 4]#^+	success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	1632	168	1c 19 00 00 00 00 00 00 05 00 00 fd 08 00 00 00 00 00 00 00 00 00 00 00 fd 14 fd 00 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 04 00 5e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 4e 16 00 00	^N	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	8574	20	11 00 00 00 00 fd 5d 00 00 00 00 00 00 40 00 00 fd 22 00 00	]@"	success or wait	17	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	8850	16384	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 5d 00 fd fd 4c 77 fd fd 5d 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd fd fd 5d 00 00 00 00 00 fd 34 4a 77 fd fd 5d 00 6c 1e 5e 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 01 33 4a 77 fd fd 5d 00 fd fd fd fd 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd 54 fd 5d 00 1a 2f 4a 77 fd fd 5d 00 fd fd 5d 00 48 fd 5d 00 44 fd 5d 00 1c fd 5d 00 24 fd 5d	]Lw]]4Jw]l^3Jw]T]/Jw]]H]D]]$]	success or wait	16	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	40374	1104	fd fd 4c 77 fd fd 4a 77 fd 00 00 00 fd fd fd fd 10 00 00 00 44 fd fd 00 10 fd fd 00 fd fd fd fd 40 fd 4a 77 40 fd 4a 77 fd fd fd fd 00 fd 67 00 00 fd 67 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd 67 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 30 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 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 04 fd 00 00 00 00 00 00 00 00 00 fd 7f fd 00 00 fd 67 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 60 fd fd 00 54 fd 67 00 68 fd fd 00 60 fd fd 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	LwJwD@Jw@Jwggg0g`Tgh`	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	6426	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 14 fd 00 48 fd 5d 00 00 00 00 00 fd 14 fd 00 fd fd fd 20 00 00 00 34 fd 5d 00 fd 14 fd 00 23 00 00 00 02 02 01 00 08 00 5e 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++H] 4]#^+	success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	1900	48	40 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 10 68 00 00 00 00 00 fd fd fd 00 00 00 00 00 6c 04 00 00 fd 62 00 00 fd 02 00 00 fd 1e 00 00	@ hlb	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	1960	4	16 00 00 00		success or wait	22	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	5026	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	22	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	4232	120	00 00 fd 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 14 16 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 0c 00 00 00 18 00 00 00 01 00 00 00	t`A!-aBB?#@A	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	5676	34	1c 00 00 00 42 00 4a 00 70 00 33 00 61 00 55 00 76 00 72 00 74 00 39 00 2e 00 64 00 6c 00 6c 00 00 00	BJp3aUvrt9.dll	success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	4352	668	00 00 fd 00 00 00 00 00 00 fd 06 00 35 fd 07 00 07 46 fd 3e 2c 16 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 04 00 00 00 00 10 fd 02 00 00 00 00 00 10 0c 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 2f fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 00 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 05 00 00 00 00 00 32 fd 45 00 00 00 00 fd 60 5e 1a 00 00 00 00 0c 3d fd 20 00 00 00 00 7d 1a 10 01 00 00 00 00 02 fd 00 00 4a 35 01 00 fd 4f 06 00 fd fd 0a 00 fd 00 05 00 06 7f 15 00 fd 05 00 fa 38 00 fd fd 01 00 1c fd 15 00 00 00 00 00 7d fd 24 00 fd 65 04	5F>,Zb/@E`^= }J5O8}$e	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	41478	6196	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB04.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 4c 09 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 10 00 00 05 00 00 00 14 01 00 00 7e 21 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 0f 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 18 11 00 00 16 00 00 00 fd 00 00 00 04 13 00 00	L$~!`8T	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6424</Pid>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1180	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 34 00 39 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>20491</Uptime>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1232	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1322	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1382	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1436	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 39 00 37 00 37 00 36 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>52977664</PeakVirtualSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1532	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 30 00 31 00 35 00 31 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>52015104</VirtualSize>	success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1612	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 31 00 36 00 39 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>1693</PageFaultCount>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 30 00 31 00 32 00 39 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>6012928</PeakWorkingSetSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 30 00 31 00 32 00 39 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>6012928</WorkingSetSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 30 00 35 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>100552</QuotaPeakPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2016	96	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 39 00 38 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>98544</QuotaPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 36 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>19648</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 35 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>19512</QuotaNonPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2374	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 31 00 34 00 39 00 39 00 31 00 33 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>1499136</PagefileUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2460	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 31 00 35 00 30 00 37 00 33 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>15 07328</Pe akPagefileUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2562	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 31 00 34 00 39 00 39 00 31 00 33 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>1499136 </PrivateUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2642	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2696	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2736	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 39 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3968</Pid>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2830	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	2912	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 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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 38 00 35 00 33 00 30 00 30 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4853008</Uptime>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3074	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3164	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3228	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	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3286	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3390	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3478	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 34 00 36 00 33 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>46376</PageFaultCount>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 39 00 35 00 33 00 35 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>101953536</PeakWorkingSetSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3682	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 36 00 34 00 31 00 31 00 36 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>96411648</WorkingSetSize>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3778	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 37 00 39 00 32 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>979216</QuotaPeakPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	3906	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 39 00 30 00 39 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>909584</QuotaPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4018	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 31 00 39 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>70192</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4156	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 37 00 32 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>67200</QuotaNonPagedPoolUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4278	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 31 00 30 00 36 00 31 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>291061776</PagefileUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4370	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 38 00 36 00 30 00 34 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35860480</PeakPagefileUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4478	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 31 00 30 00 36 00 31 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>29106176</PrivateUsage>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4564	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4620	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4670	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4708	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4756	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4802	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4864	4	0d 00 0a 00		success or wait	8	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4868	2	09 00		success or wait	16	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	4872	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	8	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	5474	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	5478	2	09 00		success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	5480	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	5520	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	5524	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	5526	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	5564	4	0d 00 0a 00		success or wait	6	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	5568	2	09 00		success or wait	12	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	5572	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6126	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6130	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6132	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6172	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6176	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6178	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6216	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6220	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6224	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6318	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6322	2	09 00		success or wait	2	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6326	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 76 00 67 00 67 00 6c 00 74 00 77 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>vggltw, Inc.</SystemManufacturer>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6432	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6436	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6440	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 76 00 67 00 67 00 6c 00 74 00 77 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>vggltw7,1</SystemProductName>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6536	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6540	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6544	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6664	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6668	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6672	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 30 00 31 00 34 00 38 00 31 00 33 00 36 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>1610148136</OSInstallDate>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6754	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6758	2	09 00		success or wait	2	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6762	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6864	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6868	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6872	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6940	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6944	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6946	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6986	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6990	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	6992	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7026	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7030	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7034	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7130	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7134	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7136	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	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7178	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7202	4	0d 00 0a 00		success or wait	3	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7206	2	09 00		success or wait	6	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7210	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7462	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7466	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7468	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7494	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7498	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7500	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 31 00 37 00 54 00 31 00 38 00 3a 00 30 00 30 00 3a 00 33 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-17T18:00:36Z">	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7600	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7604	2	09 00		success or wait	2	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7608	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 33 00 39 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 34 00 32 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 30 00 33 00 31 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 30 00 33 00 31 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="397" PID="6424" UptimeMS="6031" TimeSinceCreationMS="6031" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7870	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7874	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7878	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7898	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7902	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7904	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7942	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7946	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7948	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7986	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7990	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	7994	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 32 00 36 00 34 00 35 00 39 00 62 00 63 00 2d 00 66 00 66 00 36 00 62 00 2d 00 34 00 31 00 30 00 35 00 2d 00 39 00 35 00 34 00 61 00 2d 00 66 00 61 00 65 00 39 00 31 00 38 00 64 00 36 00 34 00 39 00 37 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>726459bc-ff6b-4105-954a-fae918d64973</Guid>	success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	8092	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	8096	2	09 00		success or wait	2	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	8100	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 31 00 37 00 54 00 31 00 38 00 3a 00 30 00 30 00 3a 00 33 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-17T18:00 :36Z</CreationTime>	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	8198	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	8202	2	09 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	8204	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	8244	4	0d 00 0a 00		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8F.tmp.WERInternalMetadata.xml	8248	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	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1046.tmp.xml	0	4558	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 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b75bd23440526356a090f9cb45508f9dce6e86_7cac0383_1ada168d\Report.wer	0	2	fd fd		success or wait	1	6DDE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b75bd23440526356a090f9cb45508f9dce6e86_7cac0383_1ada168d\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	147	6DDE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b75bd23440526356a090f9cb45508f9dce6e86_7cac0383_1ada168d\Report.wer	9020	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 31 00 30 00 34 00 32 00 31 00 34 00 39 00 32 00	MetadataHash=-110421492	success or wait	1	6DDE497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{53d2bae6-3c16-f99b-5882-f8f274ac6b90}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DE036BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	A5 01 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 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	05 00 00 C0 08 00 00 00 00 00 00 00 00 EE 14 85 00 02 00 00 00 01 00 00 00 04 00 5E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6DE01FE8	RegSetValueExW

Disassembly

No disassembly