ID: 620693
Sample Name: qjrOWCCE58
Cookbook: default.jbs
Time: 05:39:04
Date: 05/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

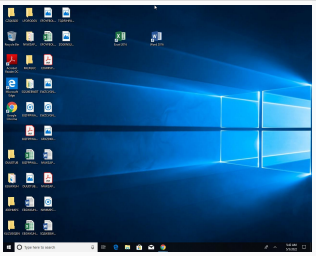
Windows Analysis Report

qjrOWCCE58

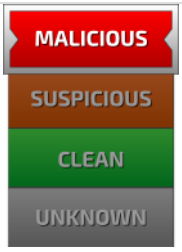
Overview

General Information

Sample Name:	qjrOWCCE58 (renamed file extension from none to exe)
Analysis ID:	620693
MD5:	732132623989ca..
SHA1:	e493be600aa8ec..
SHA256:	32f431ba791fcd1..
Tags:	32 exe trojan
Infos:	



Detection



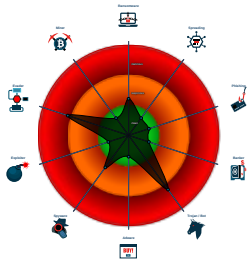
Nymaim

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Nymaim
- Multi AV Scanner detection for subm…
- Machine Learning detection for sam…
- Uses 32bit PE files
- One or more processes crash
- PE file contains strange resources
- Contains functionality to check if a d…
- Contains functionality to query local…
- Contains functionality to read the PE…
- Uses code obfuscation techniques (…
- Checks if the current process is bei…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- qjrOWCCE58.exe (PID: 1592 cmdline: "C:\Users\user\Desktop\qjrOWCCE58.exe" MD5: 732132623989CAAE367E0878298B7E9B)
  - WerFault.exe (PID: 4856 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1592 -s 656 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4412 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1592 -s 772 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3152 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1592 -s 796 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4228 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1592 -s 628 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4856 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1592 -s 900 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6220 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1592 -s 908 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6408 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1592 -s 916 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - cmd.exe (PID: 6492 cmdline: "C:\Windows\System32\cmd.exe" /c taskkill /im "qjrOWCCE58.exe" /f & erase "C:\Users\user\Desktop\qjrOWCCE58.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - taskkill.exe (PID: 6612 cmdline: taskkill /im "qjrOWCCE58.exe" /f MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.323501836.0000000000820000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
00000000.00000000.269341375.0000000000400000.00000040.00000001.01000000.00000003.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000000.00000000.283327894.0000000000820000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
00000000.00000000.262759789.0000000000820000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
00000000.00000000.253715249.0000000000400000.00000040.00000001.01000000.00000003.sdmp	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.qjrOWCCE58.exe.400000.11.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
0.0.qjrOWCCE58.exe.400000.21.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
0.0.qjrOWCCE58.exe.400000.5.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
0.0.qjrOWCCE58.exe.820e67.2.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
0.0.qjrOWCCE58.exe.400000.1.raw.unpack	JoeSecurity_Nymaim	Yara detected Nymaim	Joe Security	
Click to see the 58 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

E-Banking Fraud

Yara detected Nymaim

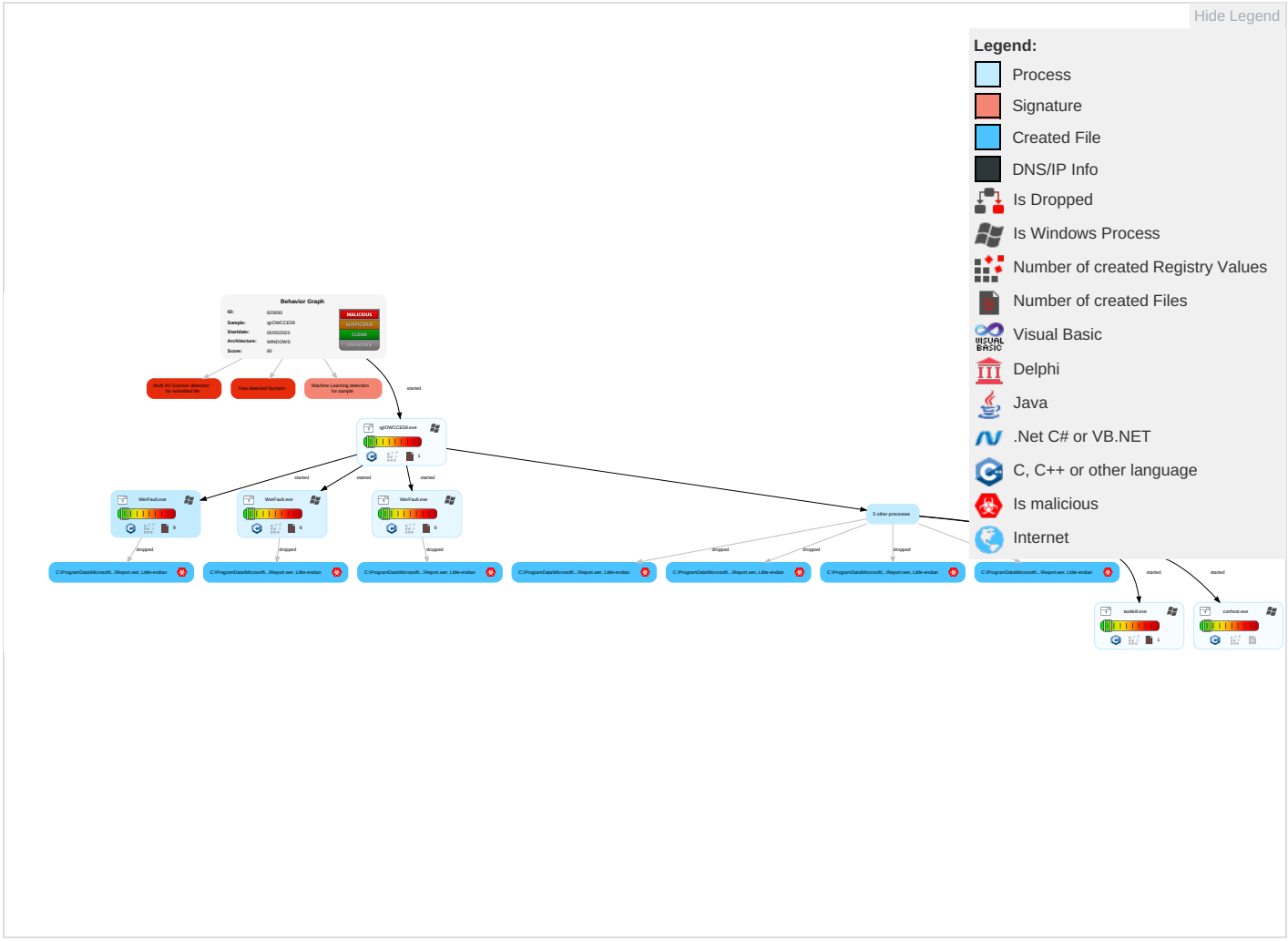
Stealing of Sensitive Information

Yara detected Nymaim

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 Process Injection	1 Disable or Modify Tools	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Virtualization/Sandbox Evasion	LSASS Memory	5 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 1 Process Injection	Security Account Manager	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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 Application Window 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	2 Obfuscated Files or Information	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	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	2 3 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

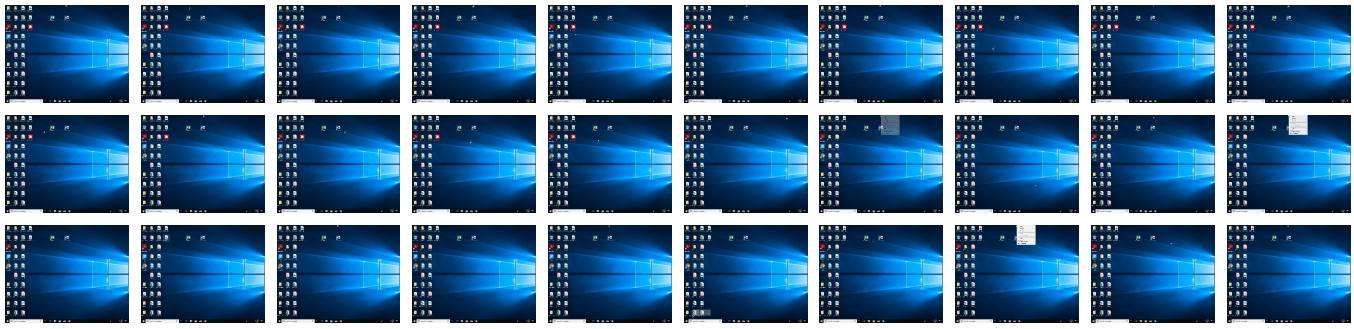
Behavior Graph



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
qjrOWCCE58.exe	34%	Virustotal		Browse
qjrOWCCE58.exe	50%	ReversingLabs	Win32.Trojan.DanaBot	
qjrOWCCE58.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620693
Start date and time: 05/05/202205:39:04	2022-05-05 05:39:04 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qjrOWCCE58 (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	43
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:	mal60.troj.evad.winEXE@12/28@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 51.8% (good quality ratio 48.9%) • Quality average: 77.1% • Quality standard deviation: 28.4%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, UpdateNotificationMgr.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 40.127.240.158, 23.205.181.161
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, arc.msn.com, ris.api.iris.microsoft.com, e11290.dspg.akamaiedge.net, go.microsoft.com, store-images.s-microsoft.com, login.live.com, go.microsoft.com.edgekey.net, sls.update.microsoft.com, settings-prod-neu-1.northeurope.cloudapp.azure.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, atm-settingsfe-prod-geo.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Copyright Joe Security LLC 2022

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_0c0c0928\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):	0.8772016254471042
Encrypted:	false
SSDEEP:	96:jKvwRjshloA7RC6tpXIQcQnc6rCcEhcw3r7+HbHg/opAnQ0DFE8WpB72OyEmBDIA:zIH56rwjxlk/u7sAS274It5E
MD5:	0216CA3E9CF45AFE94BDF4E6699D8541
SHA1:	A51A03BB633277DC82DC3F632BD7E6A50E6E5B22
SHA-256:	1DE57D9092695FC73A27B70217074D422AC9D791E60F4EA29C8DB4B3D6FA7576
SHA-512:	5B559DC0F0B1A7331653B5C3DB88C1ECD6A88AB721C79829CD2F57034F4AD1CD120BE7A79D1B91830228BA1FF26E73D982B284C81A495399FF41911BE80A7E12
Malicious:	**true**
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.=.1.3.2.9.6.2.2.8.0.1.8.8.6.5.2.1.4.7.....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.=.a.4.2.d.f.8.d.0.-.b.3.1.6.-.4.7.9.4.-.8.b.d.0.-.4.2.6.a.e.4.e.1.2.8.a.6.....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.=.1.5.f.6.4.a.a.1.-.0.8.1.e.-.4.e.e.7.-.9.8.a.5.-.8.f.e.d.6.0.a.8.3.3.8.f.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.q.j.r.O.W.C.C.E.5.8...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.6.3.8.-.0.0.0.1.-.0.0.1.d.-.2.8.b.7.-.0.6.4.0.7.d.6.0.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.4.e.4.4.7.7.f.f.5.f.3.1.1.8.6.1.4.0.f.8.1.d.f.1.1.b.b.c.e.d.5.0.0.0.0.f.f.f.f.!.0.0.0.0.e.4.9.3.b.e.6.0.0.a.a.8.e.c.f.7.3.8.4.a.c.3.f.2.3.4.5.4.d.a.f.6.f.d.d.1.8.2.1.d.!.q.j.r.O.W.C.C.E.5.8...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././.0.4././.0.6.:.2.1.:.1.3.:.4.2.!.0.!.q.j.r.O.W.C.C.E.5.8...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_10d822ca\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):	0.8774171114093317
Encrypted:	false
SSDEEP:	96:4XwR7shloA7RC6tpXIQcQnc6rCcEhcw3r7+HbHg/opAnQ0DFE8WpB72OyEmBDliX:rAH56rwjxlk/u7sbS274It5E
MD5:	5908259C5D9F1A295C347370C64591A6
SHA1:	73888E8FF847D515DE63B6072ADF8300979C7608
SHA-256:	171CF4E9AC017B0646ED2860297784CB0FFEC643B2086D9B04B7862294C1CA07
SHA-512:	DE2377A1E4FDF3F7C682709870A15E8226F0D4CA585185BA39B324DCAE7236E42D0C53A33215083EB41806991C0CEA3D01D34346596D882D1F46921E2B6A45E
Malicious:	**true**
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.=.1.3.2.9.6.2.2.8.0.2.5.6.0.8.6.5.7.4.....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.=.4.6.8.c.1.7.a.f.-.c.4.8.8.-.4.b.d.5.-.a.0.1.2.-.d.2.8.6.d.3.f.8.3.0.4.0.....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.e.9.5.2.3.d.8.-.c.5.a.2.-.4.6.9.5.-.a.6.c.8.-.e.e.a.d.d.6.b.2.8.0.f.f.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.q.j.r.O.W.C.C.E.5.8...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.6.3.8.-.0.0.0.1.-.0.0.1.d.-.2.8.b.7.-.0.6.4.0.7.d.6.0.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.4.e.4.4.7.7.f.f.5.f.3.1.1.8.6.1.4.0.f.8.1.d.f.1.1.b.b.c.e.d.5.0.0.0.0.f.f.f.f.!.0.0.0.0.e.4.9.3.b.e.6.0.0.a.a.8.e.c.f.7.3.8.4.a.c.3.f.2.3.4.5.4.d.a.f.6.f.d.d.1.8.2.1.d.!.q.j.r.O.W.C.C.E.5.8...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././/.0.4.//.0.6.:.2.1.:.1.3.:.4.2.!.0.!.q.j.r.O.W.C.C.E.5.8...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_1167fbca\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):	0.8635490173780485
Encrypted:	false
SSDEEP:	96:mYnV7wR/shloA7RC6tpXIQcQnc6rCcEhcw3r7+HbHg/opAnQ0DFE8WpB72OyEmBz:TykH56rwjxG/u7sAS274It5E
MD5:	BB701F9255E239DB0F27AEBC3EE53D43
SHA1:	C0013B523C5EAB7AE8A96E6167EBDA6A44FAC869
SHA-256:	A71EDC6B9168FD01EE055970FAE22F5592FF32CE62CC36F6BC42E64939DAFF90
SHA-512:	D8E9EDDEB2A917853F53D06DD7D1BA29F265000F4883DE1AF51086418C73A88AFF516B118D2CAA9B859C99E8B2DC0A17311AF099A08FB830EF8A5CBAA46DC26A
Malicious:	**true**
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.=.1.3.2.9.6.2.2.8.0.1.5.6.9.4.2.2.8.0.....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.=.0.0.2.c.4.7.3.d.-.5.f.8.b.-.4.3.2.7.-.9.d.d.8.-.5.4.9.1.f.4.b.e.f.d.9.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.e.d.3.3.3.f.2.-.3.a.c.e.-.4.9.0.6.-.b.3.8.5.-.7.e.c.9.e.2.b.9.2.d.a.1.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.q.j.r.O.W.C.C.E.5.8...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.6.3.8.-.0.0.0.1.-.0.0.1.d.-.2.8.b.7.-.0.6.4.0.7.d.6.0.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.4.e.4.4.7.7.f.f.5.f.3.1.1.8.6.1.4.0.f.8.1.d.f.1.1.b.b.c.e.d.5.0.0.0.0.f.f.f.f.!.0.0.0.0.e.4.9.3.b.e.6.0.0.a.a.8.e.c.f.7.3.8.4.a.c.3.f.2.3.4.5.4.d.a.f.6.f.d.d.1.8.2.1.d.!.q.j.r.O.W.C.C.E.5.8...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././/.0.4.//.0.6.:.2.1.:.1.3.:.4.2.!.0.!.q.j.r.O.W.C.C.E.5.8...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_12a3eeab\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):	0.8570740057313196
Encrypted:	false
SSDEEP:	96:iY+wRCshloA7RC6tpXIQcQnc6rCcEhcw3r7+HbHg/opAnQ0DFE8WpB72OyEmBDIM:BxH56rwjxy/u7sAS274It5E
MD5:	94FA62DE2DE6A2AF49D88BF565602D1B
SHA1:	A3DDD7742A08DEE39F5064A1EC80DB5DDCAAA07F
SHA-256:	6832FFEDEF3322E192569B7E264B8A4D8D4C1E01BA704C5D025835A1F75CBADB
SHA-512:	07ADC777F99603B2879772BED904624DF471BD48B7DB475D4EA8B921CAF3330FF6797FCFEDAE4A786EC2218F1D9EDAF3C5649373863BD3815B86D8C48465AE2
Malicious:	**true**
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.=.1.3.2.9.6.2.2.8.0.1.1.8.8.7.2.3.5.0.....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.=.4.b.a.1.3.2.3.6.-.b.d.1.1.-.4.9.5.3.-.b.1.c.7.-.2.1.2.8.8.1.c.9.e.9.d.6.....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.=.c.3.b.1.a.3.b.c.-.2.0.9.3.-.4.c.c.7.-.9.a.6.c.-.7.c.4.c.a.1.6.f.a.5.f.c.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.q.j.r.O.W.C.C.E.5.8...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.6.3.8.-.0.0.0.1.-.0.0.1.d.-.2.8.b.7.-.0.6.4.0.7.d.6.0.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.4.e.4.4.7.7.f.f.5.f.3.1.1.8.6.1.4.0.f.8.1.d.f.1.1.b.b.c.e.d.5.0.0.0.0.f.f.f.f.!.0.0.0.0.e.4.9.3.b.e.6.0.0.a.a.8.e.c.f.7.3.8.4.a.c.3.f.2.3.4.5.4.d.a.f.6.f.d.d.1.8.2.1.d.!.q.j.r.O.W.C.C.E.5.8...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././/.0.4.//.0.6.:.2.1.:.1.3.:.4.2.!.0.!.q.j.r.O.W.C.C.E.5.8...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_12a4344f\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):	0.8772900520367355
Encrypted:	false
SSDEEP:	96:+4wRDshloA7RC6tpXIQcQnc6rCcEhcw3r7+HbHg/opAnQ0DFE8WpB72OyEmBDIi8:4oH56rwjxlk/u7sbS274It5E
MD5:	B1CF46361A43EE1319E9A672595A659C
SHA1:	DB305FB5E990C87607DC31B117F2E406F76C4673
SHA-256:	9C4773A62BFDA7D66E522233163F2D69CFC213A2E20D2B5F1D82DC02C9D312C9
SHA-512:	71941E6ED1E5C5AD2BE6A887E79F0BE73259813C3F7949F1DF57EB3E519582B0989D7DC26613576D2C68B971F7AF6C2BB2775C4A5DA0D370BD2D8D7B69DBE0B
Malicious:	**true**
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.=.1.3.2.9.6.2.2.8.0.2.9.4.1.8.9.7.1.6.....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.=.7.a.d.6.7.f.b.7.-.2.d.2.3.-.4.f.a.5.-.9.6.b.c.-.9.4.c.7.2.f.d.2.5.f.e.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.1.0.5.a.a.4.a.-.4.9.9.a.-.4.9.6.2.-.a.f.5.f.-.a.6.1.0.e.c.6.a.1.f.d.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.=.q.j.r.O.W.C.C.E.5.8...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.6.3.8.-.0.0.0.1.-.0.0.1.d.-.2.8.b.7.-.0.6.4.0.7.d.6.0.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.4.e.4.4.7.7.f.f.5.f.3.1.1.8.6.1.4.0.f.8.1.d.f.1.1.b.b.c.e.d.5.0.0.0.0.f.f.f.f.!.0.0.0.0.e.4.9.3.b.e.6.0.0.a.a.8.e.c.f.7.3.8.4.a.c.3.f.2.3.4.5.4.d.a.f.6.f.d.d.1.8.2.1.d.!.q.j.r.O.W.C.C.E.5.8...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././.0.4././.0.6.:.2.1.:.1.3.:.4.2.!.0.!.q.j.r.O.W.C.C.E.5.8...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_181043fe\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):	0.8774641034858449
Encrypted:	false
SSDEEP:	96:L9DCwRnshloA7RC6tpXIQcQnc6rCcEhcw3r7+HbHg/opAnQ0DFE8WpB72OyEmBDG:Z7sH56rwjxlk/u7sbS274It5E
MD5:	76B53D6054B18CA6052DD3B136605B63
SHA1:	50E9777517AF88BA0F6CD0242CB97CC615BF37CD
SHA-256:	9DA5119CD79312E876922C812BCD73D739A71F4FAC43525D30DE77BF67088F5B
SHA-512:	65650A0FDFAF8D1F973D40173E46A348188FF04ED2C2F4DCBCA0A63A6D3053D7E7D0BAA9DB249005FE74D9B84A1FA57F8CAE5B9CAF7BA5782535A6034294A479
Malicious:	**true**
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.=.1.3.2.9.6.2.2.8.0.3.4.0.2.4.7.9.1.4.....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.=.1.a.2.a.a.d.6.2.-.3.a.9.8.-.4.3.1.f.-.b.f.d.6.-.2.4.9.d.9.0.8.c.5.d.a.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.4.6.0.a.1.7.3.-.5.c.f.a.-.4.b.f.2.-.b.8.b.f.-.1.4.9.7.b.b.5.f.c.a.3.6.....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.=.q.j.r.O.W.C.C.E.5.8...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.6.3.8.-.0.0.0.1.-.0.0.1.d.-.2.8.b.7.-.0.6.4.0.7.d.6.0.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.4.e.4.4.7.7.f.f.5.f.3.1.1.8.6.1.4.0.f.8.1.d.f.1.1.b.b.c.e.d.5.0.0.0.0.f.f.f.f.!.0.0.0.0.e.4.9.3.b.e.6.0.0.a.a.8.e.c.f.7.3.8.4.a.c.3.f.2.3.4.5.4.d.a.f.6.f.d.d.1.8.2.1.d.!.q.j.r.O.W.C.C.E.5.8...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././.0.4././.0.6.:.2.1.:.1.3.:.4.2.!.0.!.q.j.r.O.W.C.C.E.5.8...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_19545302\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):	0.8776413401735936
Encrypted:	false
SSDEEP:	96:egMUrOegwRbshloA7RC6tpXIQcQnc6rCcEhcw3r7+HbHg/opAnQ0DFE8WpB72Oy2:QIZpgH56rwjxlk/u7sbS274It5E
MD5:	070C32C8479C605B623585A13C8B68EB
SHA1:	2B1F34717D17B838EB638F65BB19CA7F4F1A0E8D
SHA-256:	5C7C7CA72B14717D2AD99C49BC29ACC0DD383A782DC08A6F5643EFF780AD601F
SHA-512:	1A0A5F10D4945C5FC95089AFF292AD18E7B5E6DE3082E73835C6BA7945006E03542AD3476E632568A29066FC0A34F0DDFA451532EC137591EAAA74984306FCFE
Malicious:	**true**

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.=.1.3.2.9.6.2.2.8.0.3.7.4.6.9.4.2.7.1.....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.=.c.d.2.a.e.9.5.7.-.4.c.5.a.-.4.b.f.0.-.8.3.c.c.-.4.0.c.3.2.4.1.9.7.2.d.9.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.9.e.3.5.2.a.b.-.5.5.c.c.-.4.b.6.b.-.9.e.3.f.-.5.9.9.2.5.7.3.9.3.e.8.8.....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.=.q.j.r.O.W.C.C.E.5.8...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.6.3.8.-.0.0.0.1.-.0.0.1.d.-.2.8.b.7.-.0.6.4.0.7.d.6.0.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.4.e.4.4.7.7.f.f.5.f.3.1.1.8.6.1.4.0.f.8.1.d.f.1.1.b.b.c.e.d.5.0.0.0.0.f.f.f.f.!.0.0.0.0.e.4.9.3.b.e.6.0.0.a.a.8.e.c.f.7.3.8.4.a.c.3.f.2.3.4.5.4.d.a.f.6.f.d.d.1.8.2.1.d.!.q.j.r.O.W.C.C.E.5.8...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.2././.0.4././.0.6.:.2.1.:.1.3.:.4.2.!.0.!.q.j.r.O.W.C.C.E.5.8...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 5 12:40:26 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	82940
Entropy (8bit):	2.419360403248699
Encrypted:	false
SSDEEP:	384:s6mU6ecPUYTpHgqPpi/bqERBqlpdBSThAIWDnHjzv4/CjkpyPWeWEj7JY5mD:b6ecF/WMqTh8HjzvCCfWqYA
MD5:	4E0FCF66325093518C5754B8F6243493
SHA1:	5D7E739936EC0E70B40DA34D2A01642A71F4CEF1
SHA-256:	AFD5DFBD711816B9342DFF86C7348BF59C63B68E859619FD47B1E4E87FD7EFD9
SHA-512:	E39E1CD548ABA5B7A0223DDF659CB6271FB56DF3368C514DBC43F757052E3085E53B403E22CC06F0D92A4480D7068096F23C9099014619D2A2DD6A9B7F06307
Malicious:	false
Preview:	MDMP..... .....sb.....T.....\.....$....6.....T.....8.....T..... ...#.....@.....,.....U.....B.....GenuineIntelW.....T.....8.....sb.....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\WER20D7.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):	8412
Entropy (8bit):	3.704836972955608
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiXc6IxS5W6YWb/SUzgN0gmfwS3CpBst89brAsfv5m:RrlsNis6IxUW6YySUzY0gmfwS5KrTfM
MD5:	7085203A35DC3F534F0CFF1B5DF0FCA3
SHA1:	D042062D778DB9348191AD2DCEC1F29641742F63
SHA-256:	5993C8A99127D2A29A30451E9AAAD4706E24B7FD0BE3B54083CDE98F5437F901
SHA-512:	EE2DCAC8978A2257CD2AD7325961D719B09C8D5B64F3D23F86F3D380E5AA5B51F8BF35BDF604B9EF9FEC88DF08008FBAE9E8F9490094B180FE56C6D0CDB69A84
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.>.1.5.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER21C3.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4704
Entropy (8bit):	4.48799041622298
Encrypted:	false
SSDEEP:	48:cvIwSD8zsGJgtWI9HyyWgc8sqYjk8fm8M4JyHMFv+q8vyHo/S4Jd:uITfcAyTgrsqYdJgmKgoa4Jd
MD5:	34269584E7C2B1D28C88F6732EDBB4CB
SHA1:	103DEA433C10D1980550EEB729B0126022AD63C9
SHA-256:	EE80EFE834063051A84E112675EE65874C298CA024D0706F1E1B15947246E2FE
SHA-512:	1267EE7F557D114CAC216CAC44EA30D4A12F0B53F6DF80EB36920D3210A30B912227C20933622B21247A5E84CF5BB3B906C05CF3A0DEDC04294EDAF92F401CA9
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="1501791" />.. <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\WER2CBD.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 5 12:40:29 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	95754
Entropy (8bit):	2.1014195071277935
Encrypted:	false
SSDEEP:	384:EdwxNWLO61K1Uev9NLbqTQKtRBqcHty8B/kP/jFvv5C470lZ/ajkpyPWeWkzvmhg:Ede61IBlcPp//kP7Fvv444ldafWvhz1m
MD5:	8652497299CC88D253E189BDA49347C7
SHA1:	50815BC9188FD0C247F2AF445B230E652D0292E4
SHA-256:	1FFA07D955164F3774F359A1AB6C0C20FC390AD1B572E70C5D99ED24A6BAA2A5
SHA-512:	DDDE030B173694723F9AA89A37FFA3BE1F8D5FE486A4C944727894E938452C5CA7944D2898458C0B3FDCC90FCA192A2B8E2C0ADE7430D814C56E8617710D598
Malicious:	false
Preview:	MDMP..... .....sb.....$....?.....T.....8.....T..... "...S.....U.....B.....T.....GenuineIntelW.....T.....8.....sb.....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\WER30D5.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):	8414
Entropy (8bit):	3.703610859341354
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiX+6Ieb6YWzSUOmBgmfwS3CpBD89bsAsfSkm:RrlsNiO6Ieb6YCSUOmBgmfwSZsTfg
MD5:	3A2AA5F63253BA9EBEA737429B82DAA0
SHA1:	7A85E6BA966635D49F62A5A64ECA1B7165129762
SHA-256:	ED50048D4D995BC2D3333C64C7BAF1FBBF40C8CD531A58638002EF9257138D1D
SHA-512:	01BBD7F42C3BE9C95BCD013DD21E1DFEE38E33EB200F2B77C3AE0A1D7C3D6F30CA9DF5DEBFB5631834E7BF32E8EB60D6AD6300EDC2815F7B31B418405EAABC07
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.>.1.5.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER329B.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4704
Entropy (8bit):	4.486722835348809
Encrypted:	false
SSDEEP:	48:cvIwSD8zsGJgtWI9HyyWgc8sqYjps8fm8M4JyHMF/+q8vyHo/S4Jd:uITfcAyTgrsqYtRJgGKgoa4Jd
MD5:	8D18C1B5C512A092175BDA8130A6F991
SHA1:	C6C36B275556769E12E2545FBFB3108FA89F9BDB
SHA-256:	0A108533A20E56651B9A4421D6227A6056EB9DED3EEE65D79BB6249F1729BC16
SHA-512:	1D3F8E48E6056D162541430BE7803158BB4F007A8D0FBDA18EEDBEBAFDF9A89F02B6A9ECA67B6237A4DCECCD1A3429AFC7DA3792AFB1A7FFB64FC19F3C593717
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="1501791" />.. <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\WER38A.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 5 12:40:19 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	83752
Entropy (8bit):	2.4289512577684818
Encrypted:	false
SSDEEP:	384:SD6m46sxkWR7PqlpSYqbqTgRBq5pdBSThAIWDnHjzv4/CRkpyPWeWEzCj9uEO:SI6s37yB4c1qTh8HjzvCCJWbu
MD5:	016703E04EDCE822899541773C68F07B
SHA1:	2BB25B21E0A9A1CFEB1B4B695C07DAF9EC11BCE5
SHA-256:	CFAA27327896C69E2FAEC1768617FBF221BA6D40FB01B9FA0CE13DFCE7F845A6
SHA-512:	4701F583CB2517B8953ACAB1BEA1EFEE6FE2FD7C5DB1DDA115B70165FFFC9E3B9EF0969FAA32251A0F6906A6D20819DC2144323F21756A7861EB25309FCAFF30
Malicious:	false
Preview:	MDMP..... .....sb.....T.....\.....$....6.....T.....8.....T..... ..H&.....@.....,.....U.....B..... .GenuineIntelW.....T.....8.....sb.....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\WER3EED.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 5 12:40:34 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	95234
Entropy (8bit):	2.1152729640763837
Encrypted:	false
SSDEEP:	384:OLwxNW46l/ft3z44vgILbqTJNs8PIKyRBqAHsCP/jFvv5C470lZ/ajkpyPDeWk78:OLM6l93eOcg4iP7Fvv444ldafDW3C+S
MD5:	7E4F2ED8F56A715AD723B10F5090863D
SHA1:	46A87441A2DFDAF161D075598414E95EEE899791
SHA-256:	C72440E77E5B3EBB2BEF85BE9F3EEEE2FB3111E83BA24CEFED3C6048C3EA7BEC
SHA-512:	9E0BE163B7C7566AB082776956C5968A56605D537C2FF09FB9A6F28CE2F160F756652D095F70F01450CC7C05E4EF5ACC5C251C6A33F5E1A99A141FF06DD9214B
Malicious:	false
Preview:	MDMP..... .....sb.....D....?.....T.....8.....T..... "...Q.....U.....B.....T.....GenuineIntelW.....T.....8.....sb.....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\WER41DC.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):	8412
Entropy (8bit):	3.7025697219105487
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiX+6Ie7ub6YWzSUZNgmfwS3CpBS89blAsfNYm:RrlsNiO6Ie7ub6YCSUZNgmfwSmITfX
MD5:	351702278BFB4F913C64D7B32254E491
SHA1:	0899A811DEA171CE7E3F5EBE7E46D49196D5EED1
SHA-256:	D9CC60346ED834A1E8AA5F76E4A35F1CED6777D1D198B084EBD052CA814779E6
SHA-512:	B562AF57DF19E7CFD43954358861A51812F96D3CAEA23434198BA42A7E21B280D0782B3504029985244B54D63839D24A5B50C0E985F3ADF02ECB69C5BBE24782
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.>.1.5.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4306.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4704
Entropy (8bit):	4.490571287892598
Encrypted:	false
SSDEEP:	48:cvIwSD8zsGJgtWI9HyyWgc8sqYjz8fm8M4JyHMF+z+q8vyHo/S4Jd:uITfcAyTgrsqY0JgxzKgoa4Jd
MD5:	B1309460E6A3530F0CD91114E1BEE2EB
SHA1:	344C5167F32E869AA43805F5F9EB44475787EEA4
SHA-256:	B6ABBCA54DF7EC1DBF6E8179D778719D6F13D4D1D34E85CBAC9BE053215E25AF
SHA-512:	11532CA3CA48244009ABC4D2A8EC502C01DA47E075BF7D4A7173DE22699B86CB321BB3A04CDBE6CD2B2D7C14CDC78A802FCE7BD509A64F180304D5AABE33 5DC
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="1501791" />.. <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\WER4C2C.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 5 12:40:38 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	95266
Entropy (8bit):	2.1510015050081264
Encrypted:	false
SSDEEP:	768:+A3n6XSLfzolcJP7Fvv444ldafW4YUs8:/bboIPpvvaldafW4YUs8
MD5:	1E7B0A782E7E255A743111106FDA01F4
SHA1:	6E503317B9AB2A60DFB2E687FF18DAF139CE53CC
SHA-256:	C479C1B148A74FC7C8761127F3A73A0E67CA072FB604B12A7072B360440344F5
SHA-512:	5293826821F8880AE5EB98DDA8DC236DB88916586F925A7494FE39812222CD521E2843156D2F78063FCFC7405630796A7494C6D4E89CBB367312B7E0A360A197
Malicious:	false
Preview:	MDMP..... .....sb.....D....?.....T.....8.....T.....".Q.....U.....B.....T.....GenuineIn telW.....T.....8.....sb.....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\WER5015.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):	8414
Entropy (8bit):	3.703074171870118
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiXi6IeT+6YWrSUCmwgmfwS3CpBE89b0Asf3D8m:RrlsNiy6Ieq6YKSUCmwgmfwSM0Tf3d
MD5:	E5E79DB734B573FC3D62A2FAB266D0D1
SHA1:	31CD7AE4F6A2D6F15CB35983C8AD85ABA35C71A3
SHA-256:	CB8C4E7222E59391ED027F7640B5EF16EC3B7A6F65D9D90E3DA666A1C9F3D855
SHA-512:	626F022F6712ADE4A93846A76949C3F49DD47D67E83630E78FB2F44EE495D5C97C539927C9DA928FC96AE646835FDC032AF5D874841D9C732FE63610DB17B80I
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.>.1.5.9. 2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER51AC.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe

File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4704
Entropy (8bit):	4.491275091994293
Encrypted:	false
SSDEEP:	48:cvIwSD8zsGJgtWI9HyyWgc8sqYj2O/8fm8M4JyHMFV+q8vyHo/S4Jd:uITfcAyTgrsqYyrJgAKgoa4Jd
MD5:	22A9BC37AA68983F17219F8759BE6329
SHA1:	CA6670108782C1C595F25485BBE2FC85B004B990
SHA-256:	F2A900B3E240C515018C0F4107BF7C716AE4D7A8FF2EBDD7B66F6366DB383597
SHA-512:	19734112F4D25A5070ECFC1F0F6C3C8EFB60AC99E38602C5F63B3048B10609997BDAD1C776DBFB06F829E2F491DA7286F9A8E4EF5AE288950F63A1B4366D0B2B
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="1501791" />.. <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\WER63B.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):	8414
Entropy (8bit):	3.7024272119958797
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiXd6IxLHv6YWwSUWmggmfwS3CpB889bfAsf0sVm:RrlsNit6IxTv6YhSUWmggmfwS0fTf2
MD5:	5499AA13B33AAC94867AB8E7FE331230
SHA1:	EA921C47B6FD21F988AB0B3EB2B6C19B5C3979E3
SHA-256:	2A5BB51D3D4DA337239661BB858E5ED8188BC2E2A9F22FEAA12C21D7AC7F1A0B
SHA-512:	1CEB67E0CD7684E3FBF5B9639C4F28448A803273DD331C7DF59B771C67A06AE2E91525DCC6A0FF755C046CB9A252A9181D243B53004C333E2BFD613FAF291C0
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.>.1.5.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER774.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4704
Entropy (8bit):	4.486743778621484
Encrypted:	false
SSDEEP:	48:cvIwSD8zs3NJgtWI9HyyWgc8sqYjRS8fm8M4JyHMFK+q8vyHo/S4Jd:uITf3nAyTgrsqYBJgjKgoa4Jd
MD5:	FA506C2DCBE1904491B680DF01070820
SHA1:	728BE6F69194C7D0B87D04FBEA761D2A47F80622
SHA-256:	F84997D5C5577D189AF9D725F815128F6FC9B4F2370A831DDAB26FC1BF068442
SHA-512:	F20EA9B1E7372879D56C903AEC9B9CD6C662C9E1232E6EE4F741FAB525CC32B36D83C11A034514774CA282004888AB24C74F6CD02FEAA296EF6BD47692679B2C
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="1501790" />.. <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\WERE842.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 5 12:40:12 2022, 0x1205a4 type

Category:	dropped
Size (bytes):	56884
Entropy (8bit):	2.415860924030049
Encrypted:	false
SSDEEP:	192:fPKgcsg6XO6/kemPrvqTYduUPrJ0RKOmDPvCgFo5cM8V/CdNA99XoABNn/TnWAPH:Ks5+647qTaR69yPreWM8V/CduYAP3
MD5:	084523D0081F9FCB92BDB2BE918C02B4
SHA1:	D452A6850378959506A7E9DE9B32DB4B0301B014
SHA-256:	DE5096BBEC9A850DB1AB1CC02E1D4A705BC16374233272BD1C0D1876DDE39504
SHA-512:	AA31ACE0BAA48F7999C45EB9405E2CE84AA47245F0A732E12D985461B1CC8A4C74175DE90AD7D7455C074E0CFAF0AF8CC468D05965EAB3AA29DE2E0406FA44FC
Malicious:	false
Preview:	MDMP..... .....sb.....t...8,.....T.....8.....T.....p.....l.....X.....U.....B.....GenuineIntelW.....T.....8....sb.....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\WEREC5A.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):	8396
Entropy (8bit):	3.7035592860710342
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiXi67Tn6YW3SU8q8EGgmfwS3CpB189blAsffXm:RrlsNiS6f6YWSU8qWgmfwS/ITfe
MD5:	042D67A49C3B904D8EC80BFBCA455927
SHA1:	94D0F9197194061DD0A56F87CE23A447E22D7E3D
SHA-256:	1903C1E93B0B51E4B2E180D790BA2B0A257615046793D41072001E52BDD3356F
SHA-512:	E36325D464D6DB3C45DD759BAA5B58E39ED866F18F87A864C2D1A8FB5F34EBEAAB4822EA8A187B9A457C95B3B024DF373B70303BFE96510A1D40F0ACF0DE889F
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.>.1.5.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERED84.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4704
Entropy (8bit):	4.48831411399447
Encrypted:	false
SSDEEP:	48:cvIwSD8zs3NJgtWI9HyyWgc8sqYjD8fm8M4JyHMF7+q8vyHo/S4Jd:uITf3nAyTgrsqYcJgyKgoa4Jd
MD5:	2013DBBC396E4181584618890D6303E5
SHA1:	6242779877B071CB5671ECDF90B6001A8CB50024
SHA-256:	51B5503DCB1AC878B6F684FEA0592C9A3207167DC33A3562471D3879C1963139
SHA-512:	8CACB344D009BA19CC292A7D72652EB64671AFD2EB2E12EF3CC46F56567212005EF24FB8DAF1C721260CB1B1B89A32270C8A3FEDF220ADC9ACDB72EB446873F
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="1501790" />.. <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\WERF726.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 5 12:40:16 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	66184

Entropy (8bit):	2.4170302037551803
Encrypted:	false
SSDEEP:	384:nhA6LAuRhVz7qTWRHmAT6cgoypOWkHfZwHyPreWoGbNc6oq:W6LzRTcCOJpTkHf/rTcX
MD5:	03152090D258B31B0A5841B5F8DE9894
SHA1:	6148F0F788B953E99BE2ED87F5F576780540AFC8
SHA-256:	D314B293B63F3317BC57C229001786D52B211C4713718A2D07AB61870430B532
SHA-512:	9F01EE60A270631BE9C611833FE93371AA5889928EB4729E53291C125E1E68CA380C9E1948D190A4709A3BCC1E629D667C293C3B0CCAB337EDAEF7BE41F88E6E
Malicious:	false
Preview:	MDMP..... .....sb.....T.../.....T.....8.....T.....U.....B.....GenuineIntelW.....T.....8.....sb.....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\WERF9A8.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):	8408
Entropy (8bit):	3.7054266064062933
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiX56l6YWISUcmqgmfwS3CpBK89b4AsfAIm:RrlsNip6l6YpSUcmqgmfwSe4TfW
MD5:	A035334EC161C6D7F5680C9A8DA9E44E
SHA1:	C1FBBCDBFA56F9C9793687E7E9E4E07D04CBE7B5
SHA-256:	A52129FD48EA1899AEA1136E9EA74D7CF6DCE8799488892BE8E16B99DF137145
SHA-512:	399CA2D36E67F88EB86BBFC135C5D12FD5646E9BD54B08F9A96EDFB51F93CAF39002D6338B8BC69152071087A73E79B265ABB0A63C5B8C6D65553F3E3C33B0A
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.>.1.5.9.2.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAD2.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4704
Entropy (8bit):	4.488609169147605
Encrypted:	false
SSDEEP:	48:cvIwSD8zs3NJgtWI9HyyWgc8sqYjeBb8fm8M4JyHMFHD+q8vyHo/S4Jd:uITf3nAyTgrsqYSBYJgsDKgoa4Jd
MD5:	4AF206325FCB38DF334DC89D2E124161
SHA1:	56A544ABC7059C20AFAE962EE400AF6BA82681F3
SHA-256:	9AFB525540C42E4FD140FF4833FA4CCCCEAC223F91909863883732E00CE334B1
SHA-512:	1742F305A72484C29C15B6C5755A31C1D41D789A7C9D2C46B205646B8C08E9A9376592B2D58E8D0D4B2C88154A3440A6297EFE9AEAFB8996D8DD23FC8AA3C92
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="1501790" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.13596800103892

TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	qjrOWCCE58.exe
File size:	382976
MD5:	732132623989caae367e0878298b7e9b
SHA1:	e493be600aa8ecf7384ac3f23454daf6fdd1821d
SHA256:	32f431ba791fcd1f53e53b26447c9dbf59983549f567bac43ea9578b98de4ca8
SHA512:	6b98ae444381d8782ea5177694f5a5377e22f360d42bd579463f9da5c9b82cef77aa4bef489d23ca5cb6cc503e906f8231e9a79650cb79ebb5b226fd8c5c95ae
SSDEEP:	6144:SOHGuNkVVlgz8djnAv3GsrCynHcyMHwLQ9zsF2RcS3+Xyiv+Y6itQ7VsS:SihyV368djA+spnHcyMQwSS3+B+QGVs
TLSH:	DB84BE10BB90C034F5B761F48A76C3A8793EBDA19B2455CB62D43AEE66346E0EC31357
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....n...n...n...<8..n...<...n.....n...n..En...<)..n...<9..n...<<..n..Rich.n.....PE..L.....p`.....

File Icon

Icon Hash:	c6e8e8e8e8f0e461

Static PE Info

General

Entrypoint:	0x40c1b0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x6070DBE8 [Fri Apr 9 22:57:44 2021 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:	6155d4d1fe9d4982682a0787c78cb5b8

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
call 00007F2F58C86E2Bh
call 00007F2F58C79B06h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
mov edi, edi
push ebp
mov ebp, esp
push FFFFFFFEh
push 0042A518h
push 0040FE10h
mov eax, dword ptr fs:[00000000h]
push eax
add esp, FFFFFF94h
push ebx
push esi
push edi
mov eax, dword ptr [004515A4h]
xor dword ptr [ebp-08h], eax
xor eax, ebp
push eax
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
mov dword ptr [ebp-18h], esp
mov dword ptr [ebp-70h], 00000000h
mov dword ptr [ebp-04h], 00000000h
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [004010ACh]
mov dword ptr [ebp-04h], FFFFFFFEh
jmp 00007F2F58C79B18h
mov eax, 00000001h
ret
mov esp, dword ptr [ebp-18h]
mov dword ptr [ebp-78h], 000000FFh
mov dword ptr [ebp-04h], FFFFFFFEh
mov eax, dword ptr [ebp-78h]
jmp 00007F2F58C79C47h
mov dword ptr [ebp-04h], FFFFFFFEh
call 00007F2F58C79C84h
mov dword ptr [ebp-6Ch], eax
push 00000001h
call 00007F2F58C87ECAh
add esp, 04h
test eax, eax
jne 00007F2F58C79AFCh
push 0000001Ch
call 00007F2F58C79C3Ch
add esp, 04h
call 00007F2F58C7FA44h
test eax, eax
jne 00007F2F58C79AFCh
push 00000010h

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [ASM] VS2008 build 21022 • [LNK] VS2008 build 21022 • [RES] VS2008 build 21022 • [C++] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2ac0c	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x92000	0xbf20	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1310	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x8ab8	0x18	.text
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x8a70	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x2c4	.text
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	0x2acb6	0x2ae00	False	0.42072476312	data	6.17133186898	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2c000	0x65428	0x26600	False	0.96707680171	data	7.92962544889	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x92000	0xbf20	0xc000	False	0.537943522135	data	5.62006436442	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0x9c018	0x2	data	Uzbek	Italy
AFX_DIALOG_LAYOUT	0x9c010	0x2	data	Uzbek	Italy
MIMELA	0x9bc80	0x2fa	ASCII text, with very long lines, with no line terminators	Uzbek	Italy
RT_CURSOR	0x9c020	0x130	data	Uzbek	Italy
RT_CURSOR	0x9c168	0x130	data	Uzbek	Italy
RT_CURSOR	0x9c298	0xf0	data	Uzbek	Italy
RT_CURSOR	0x9c388	0x10a8	dBase III DBT, version number 0, next free block index 40	Uzbek	Italy
RT_ICON	0x92720	0x6c8	data	Uzbek	Italy
RT_ICON	0x92de8	0x568	GLS_BINARY_LSB_FIRST	Uzbek	Italy
RT_ICON	0x93350	0x10a8	data	Uzbek	Italy
RT_ICON	0x943f8	0x988	dBase III DBT, version number 0, next free block index 40	Uzbek	Italy
RT_ICON	0x94d80	0x468	GLS_BINARY_LSB_FIRST	Uzbek	Italy
RT_ICON	0x95238	0x8a8	dBase III DBT, version number 0, next free block index 40, 1st item "\251\317"	Uzbek	Italy
RT_ICON	0x95ae0	0x6c8	dBase III DBT, version number 0, next free block index 40, 1st item "\251\317"	Uzbek	Italy
RT_ICON	0x961a8	0x568	GLS_BINARY_LSB_FIRST	Uzbek	Italy
RT_ICON	0x96710	0x10a8	data	Uzbek	Italy
RT_ICON	0x977b8	0x988	data	Uzbek	Italy
RT_ICON	0x98140	0x468	GLS_BINARY_LSB_FIRST	Uzbek	Italy

Name	RVA	Size	Type	Language	Country
RT_ICON	0x98608	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4292543265, next used block 4292805161	Uzbek	Italy
RT_ICON	0x9abb0	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4292739362, next used block 4293001766	Uzbek	Italy
RT_STRING	0x9d5a0	0x16e	data	Uzbek	Italy
RT_STRING	0x9d710	0x4b8	data	Uzbek	Italy
RT_STRING	0x9dbc8	0x23c	data	Uzbek	Italy
RT_STRING	0x9de08	0x114	data	Uzbek	Italy
RT_ACCELERATOR	0x9bfb8	0x58	data	Uzbek	Italy
RT_ACCELERATOR	0x9bf80	0x38	data	Uzbek	Italy
RT_GROUP_CURSOR	0x9c150	0x14	data	Uzbek	Italy
RT_GROUP_CURSOR	0x9d430	0x30	data	Uzbek	Italy
RT_GROUP_ICON	0x9bc58	0x22	data	Uzbek	Italy
RT_GROUP_ICON	0x985a8	0x5a	data	Uzbek	Italy
RT_GROUP_ICON	0x951e8	0x4c	data	Uzbek	Italy
RT_VERSION	0x9d460	0x140	MIPSEB-LE MIPS-III ECOFF executable not stripped - version 0.79	Uzbek	Italy

Imports

DLL	Import
KERNEL32.dll	GetNamedPipeHandleStateW, CreateIoCompletionPort, FillConsoleOutputCharacterW, SetThreadAffinityMask, TerminateProcess, GetCurrentProcessId, GetVersionExA, EnumDateFormatsExW, FindNextFileW, CopyFileExA, BuildCommDCBAndTimeoutsW, DebugSetProcessKillOnExit, WriteProfileStringW, WritePrivateProfileStructA, FindFirstChangeNotificationA, MapViewOfFileEx, CreateTimerQueue, FindNextVolumeMountPointA, SetVolumeMountPointW, GetWriteWatch, ReadConsoleInputA, SetComputerNameExA, SystemTimeToTzSpecificLocalTime, GetSystemDirectoryA, GetDriveTypeW, BuildCommDCBAndTimeoutsA, LoadLibraryA, GlobalAlloc, VerifyVersionInfoW, GetBinaryTypeA, InterlockedExchange, InterlockedDecrement, FormatMessageW, SetDllDirectoryA, GetNamedPipeHandleStateA, WritePrivateProfileStringA, GetConsoleAliasesLengthW, GetProcessHeap, OpenWaitableTimerW, UnlockFile, InterlockedIncrement, GetStartupInfoW, GetSystemWow64DirectoryW, SetLastError, GetConsoleAliasExesW, ContinueDebugEvent, EndUpdateResourceA, GetLastError, FlushConsoleInputBuffer, SetDefaultCommConfigW, VirtualFree, GlobalUnfix, GetSystemWindowsDirectoryA, CopyFileA, TerminateThread, GetOEMCP, EnterCriticalSection, HeapUnlock, GetMailslotInfo, CreateActCtxA, GetConsoleAliasW, _lwrite, CreateNamedPipeA, SetSystemTimeAdjustment, DefineDosDeviceW, GetAtomNameA, SetConsoleScreenBufferSize, EnumResourceTypesA, lstrlenA, LoadLibraryW, MoveFileW, WriteConsoleA, VirtualProtect, GetModuleHandleW, ReadConsoleOutputW, GetThreadContext, BuildCommDCBW, AddRefActCtx, WritePrivateProfileStringW, GetFileAttributesW, CopyFileW, GetVolumePathNameW, GetCommMask, CloseHandle, EnumDateFormatsExA, FindActCtxSectionStringA, GetNamedPipeInfo, AttachConsole, GlobalGetAtomNameW, SetComputerNameA, GetConsoleAliasesW, WriteConsoleInputW, CreateMailslotW, SetLocalTime, EnumSystemLocalesA, CallNamedPipeA, GetConsoleAliasExesLengthW, FindActCtxSectionStringW, GetPrivateProfileIntW, GetModuleHandleExW, GetStringTypeA, GetTickCount, OpenWaitableTimerA, GlobalWire, GetCompressedFileSizeW, SetThreadPriority, MapUserPhysicalPages, WriteConsoleOutputCharacterA, EnumDateFormatsA, TerminateJobObject, CreateFileW, GetDateFormatA, FindAtomA, FindNextVolumeA, Sleep, InitializeCriticalSection, DeleteCriticalSection, LeaveCriticalSection, RaiseException, RtlUnwind, WideCharToMultiByte, HeapValidate, IsBadReadPtr, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetModuleFileNameW, GetCurrentProcess, IsDebuggerPresent, GetProcAddress, TlsGetValue, TlsAlloc, TlsSetValue, GetCurrentThreadId, TlsFree, GetACP, GetCPInfo, IsValidCodePage, SetStdHandle, GetFileType, WriteFile, GetConsoleCP, GetConsoleMode, SetHandleCount, GetStdHandle, GetStartupInfoA, QueryPerformanceCounter, GetSystemTimeAsFileTime, ExitProcess, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, HeapDestroy, HeapCreate, HeapFree, GetModuleFileNameA, HeapAlloc, HeapSize, HeapReAlloc, VirtualAlloc, FlushFileBuffers, DebugBreak, OutputDebugStringA, WriteConsoleW, OutputDebugStringW, InitializeCriticalSectionAndSpinCount, MultiByteToWideChar, GetStringTypeW, GetLocaleInfoA, LCMapStringA, LCMapStringW, GetConsoleOutputCP, SetFilePointer, CreateFileA, ReadFile
ADVAPI32.dll	ImpersonateSelf

Version Infos

Description	Data
Translations	0x0208 0x02be

Possible Origin

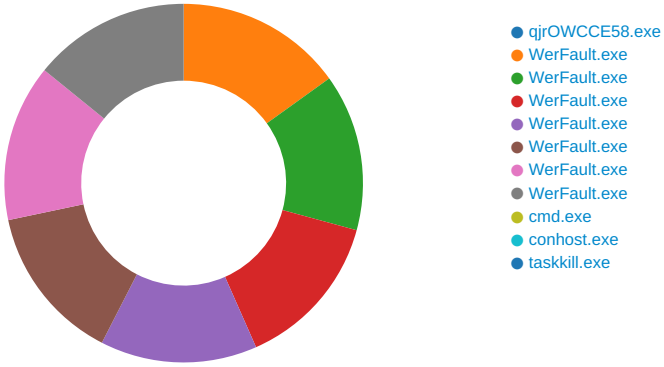
Language of compilation system	Country where language is spoken	Map
Uzbek	Italy	

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: qjrOWCCE58.exe PID: **1592**, Parent PID: **3772**

General

Target ID:	0
Start time:	05:40:06
Start date:	05/05/2022
Path:	C:\Users\user\Desktop\qjrOWCCE58.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\qjrOWCCE58.exe"
Imagebase:	0x400000
File size:	382976 bytes
MD5 hash:	732132623989CAAE367E0878298B7E9B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000002.323501836.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.269341375.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.283327894.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.262759789.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.253715249.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.280137430.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.253175312.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.302456596.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.291073585.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.283828611.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.263480015.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.284150109.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.301360286.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.302642354.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000003.250452760.0000000000860000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.254142123.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.292136739.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.301881203.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.269598460.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.262441622.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.263212749.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.309005504.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.309602192.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000002.323104838.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.309769483.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.291503648.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.270183524.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.292619266.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.252534472.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.269963050.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Nymaim, Description: Yara detected Nymaim, Source: 00000000.00000000.309168636.0000000000820000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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: **4856**, Parent PID: **1592**

General

Target ID:	2
Start time:	05:40:10
Start date:	05/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1592 -s 656

Imagebase:	0x60000
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	6FBF1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERED84.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERED84.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_12a3eeab	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_12a3eeab\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FBE497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERED84.tmp	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERED84.tmp.xml	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD9C5.tmp.csv	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD9F5.tmp.txt	success or wait	1	6FBE497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 fd fd 73 62 fd 05 12 00 00 00 00 00	MDMP sb	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	6640	6	00 00 00 00 00 00		success or wait	1	6FBE497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	200	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 19 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 38 06 00 00 fd fd 73 62 01 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	UBGenuineIntelWT8sb0Pacific Standard TimePacific Daylight Time	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	7740	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 50 fd fd 24 1c fd 75 02 00 00 00 00 00 00 40 00 50 fd fd 24 00 00 00 00 28 fd 75 02 50 fd fd 24 23 00 00 00 46 02 01 00 0c fd 75 02 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 fd	+S++P$u@P$(uP$#Fu+	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	1620	168	fd 0b 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 50 fd fd 24 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 50 fd fd 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 3c 1e 00 00	PP<	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	11320	20	27 00 00 00 18 fd 58 00 00 00 00 00 04 00 00 00 fd 2e 00 00	'X.	success or wait	39	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	11948	4	fd 7b 57 77	{Ww	success or wait	38	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	46100	4	00 00 40 00	@	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	1788	4	04 00 00 00		success or wait	4	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	8456	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 fd 7b 57 77 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd 19 00 2c fd 4c 77 23 00 00 00 12 02 00 00 70 fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++{Ww,Lw#p+	success or wait	4	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	1936	48	fd 0b 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 50 2c 00 00 00 00 00 fd fd 75 02 00 00 00 00 54 12 00 00 fd fd 00 00 fd 02 00 00 6c 29 00 00	P,uTl)	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	1996	4	25 00 00 00	%	success or wait	37	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	6646	34	1c 00 00 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 00 2e 00 65 00 78 00 65 00 00 00	qjrOWCCE58.exe	success or wait	37	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	5888	752	00 00 fd 73 00 00 00 00 00 30 08 00 6d fd 08 00 63 fd fd 0d 20 1e 00 00 fd 04 fd fd 00 00 01 00 0c 00 fd 07 00 40 fd 2a 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 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 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 60 02 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 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 3e 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6d 05 00 00 00 00	s0mc @*B? $@AZb`>@m	success or wait	1	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	46104	10780	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE842.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 0f 00 00 fd 07 00 00 05 00 00 00 74 02 00 00 38 2c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 70 1d 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 6c 17 00 00 16 00 00 00 fd 00 00 00 58 19 00 00	t8,T8TplX	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 35 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1592</Pid>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 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>qjrOWCCE58.exe</ImageName>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1084	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1182	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 30 00 35 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6055</Uptime>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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 39 00 33 00 37 00 35 00 37 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>93757440</PeakVirtualSize>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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 39 00 33 00 37 00 34 00 39 00 32 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>93749248</VirtualSize>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.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 32 00 39 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2964</PageFaultCount>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1696	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 31 00 35 00 37 00 35 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>11157504</PeakWorkingSetSize>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1794	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1798	2	09 00		success or wait	3	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1804	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 31 00 35 00 37 00 35 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>11157504</WorkingSetSize>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1886	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1890	2	09 00		success or wait	3	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	1896	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 37 00 36 00 36 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>176672</QuotaPeakPagedPoolUsage>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2010	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2014	2	09 00		success or wait	3	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2020	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 36 00 34 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>176496</QuotaPagedPoolUsage>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2118	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2122	2	09 00		success or wait	3	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2128	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 31 00 36 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>31168</QuotaPeakNonPagedPoolUsage>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2252	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2256	2	09 00		success or wait	3	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2262	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 38 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>30816</QuotaNonPagedPoolUsage>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2370	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2374	2	09 00		success or wait	3	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2380	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 35 00 36 00 36 00 30 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>2756608</PagefileUsage>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2456	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2460	2	09 00		success or wait	3	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2466	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 32 00 37 00 36 00 34 00 38 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>27764800</PeakPagefileUsage>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2558	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2562	2	09 00		success or wait	3	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2568	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 35 00 36 00 36 00 30 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>2756608</PrivateUsage>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2640	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2644	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2648	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2694	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2698	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2702	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2732	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2736	2	09 00		success or wait	3	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2742	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2782	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2786	2	09 00		success or wait	4	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2794	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2824	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2828	2	09 00		success or wait	4	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2836	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2906	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2910	2	09 00		success or wait	4	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	2918	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3008	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3012	2	09 00		success or wait	4	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3020	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 30 00 32 00 33 00 38 00 39 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6023892</Uptime>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3068	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3072	2	09 00		success or wait	4	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3080	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3158	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3162	2	09 00		success or wait	4	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3170	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3222	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3226	2	09 00		success or wait	4	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3234	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3278	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3282	2	09 00		success or wait	5	6FBE497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3292	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3382	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3386	2	09 00		success or wait	5	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3396	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3470	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3474	2	09 00		success or wait	5	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3484	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 35 00 37 00 36 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>45761</PageFaultCount>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3560	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3564	2	09 00		success or wait	5	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3574	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 32 00 30 00 32 00 33 00 31 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>102023168</PeakWorkingSetSize>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3674	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3678	2	09 00		success or wait	5	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3688	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 31 00 39 00 39 00 30 00 34 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>101990400</WorkingSetSize>	success or wait	1	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3772	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3776	2	09 00		success or wait	5	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3786	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 36 00 37 00 37 00 32 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 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>96772 8</QuotaPeakPagedPoolUsage>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3900	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3904	2	09 00		success or wait	5	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	3914	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 33 00 37 00 32 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >937280</Q uotaPagedPoolUsage>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4012	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4016	2	09 00		success or wait	5	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4026	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 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedP oolUsage>70 736</QuotaPeakNonPag edPoolUsage>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4150	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4154	2	09 00		success or wait	5	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4164	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 39 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUs age>69376< /QuotaNonPagedPoolUsa ge>	success or wait	1	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4272	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4276	2	09 00		success or wait	5	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4286	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 38 00 31 00 31 00 39 00 30 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34811904</PagefileUsage>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4364	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4368	2	09 00		success or wait	5	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4378	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 34 00 31 00 38 00 31 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35418112</PeakPagefileUsage>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4472	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4476	2	09 00		success or wait	5	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4486	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 38 00 31 00 31 00 39 00 30 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34811904</PrivateUsage>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4560	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4564	2	09 00		success or wait	4	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4572	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4618	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4622	2	09 00		success or wait	3	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4628	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4670	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4674	2	09 00		success or wait	2	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4678	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4716	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4764	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4802	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4806	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4810	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4862	4	0d 00 0a 00		success or wait	9	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4866	2	09 00		success or wait	18	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	4870	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 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>qjrOWCCE58.exe</Parameter0>	success or wait	9	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	5588	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	5592	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	5594	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	5634	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	5638	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	5640	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	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	5678	4	0d 00 0a 00		success or wait	6	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	5682	2	09 00		success or wait	12	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	5686	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6240	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6244	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6246	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6292	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6330	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6334	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6338	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6432	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6436	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6440	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 68 00 6e 00 74 00 71 00 73 00 70 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>hntqsp, Inc.</SystemManufacturer>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6546	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6550	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6554	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 68 00 6e 00 74 00 71 00 73 00 70 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>hntqsp7,1</SystemProductName>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6650	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6654	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6658	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6778	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6782	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6786	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 30 00 34 00 37 00 35 00 37 00 30 00 31 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1604757010</OSInstallDate>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6868	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6872	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6876	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6978	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6982	2	09 00		success or wait	2	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	6986	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7054	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7058	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7060	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7106	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7140	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7144	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7148	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</UEFI SecureBootEnabled>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7244	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7248	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7250	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7286	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7290	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7292	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7316	4	0d 00 0a 00		success or wait	3	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7320	2	09 00		success or wait	6	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7324	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 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7570	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7574	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7576	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7602	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7606	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7608	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 30 00 35 00 54 00 31 00 32 00 3a 00 34 00 30 00 3a 00 31 00 33 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-05T12:40:13Z">	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7708	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7712	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7716	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 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 35 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 32 00 31 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 32 00 31 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="395" PID="1592" UptimeMS="2218" TimeSinceCreationMS="2218" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7978	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7982	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	7986	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	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8006	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8010	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8012	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8050	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8054	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8056	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8094	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8098	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8102	98	3c 00 47 00 75 00 69 00 64 00 3e 00 34 00 62 00 61 00 31 00 33 00 32 00 33 00 36 00 2d 00 62 00 64 00 31 00 31 00 2d 00 34 00 39 00 35 00 33 00 2d 00 62 00 31 00 63 00 37 00 2d 00 32 00 31 00 32 00 38 00 38 00 31 00 63 00 39 00 65 00 39 00 64 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>4ba13236-bd11-4953-b1c7-212881c9e9d6</Guid>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8200	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8204	2	09 00		success or wait	2	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8208	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 30 00 35 00 54 00 31 00 32 00 3a 00 34 00 30 00 3a 00 31 00 33 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-05T12:40:13Z</CreationTime>	success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8306	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8310	2	09 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8312	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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8352	4	0d 00 0a 00		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC5A.tmp.WERInternalMetadata.xml	8356	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	6FBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERED84.tmp.xml	0	4704	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_12a3eeab\Report.wer	0	2	fd fd		success or wait	1	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_12a3eeab\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	162	6FBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_12a3eeab\Report.wer	10590	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 32 00 37 00 31 00 39 00 38 00 38 00 31 00 30 00 33 00	MetadataHash=1271988103	success or wait	1	6FBE497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	success or wait	1	6FC036BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6FC01FB2	RegCreateKeyExW
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6FBE43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	ProgramId	unicode	000604e4477ff5f31186140f81df11bbced50000ffff	success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	FileId	unicode	0000e493be600aa8ecf7384ac3f23454daf6fdd1821d	success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	LowerCaseLongPath	unicode	c:\users\user\desktop\qjrowcce58.exe	success or wait	1	6FC036BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	LongPathHash	unicode	qjrowcce58.exe|2dcf57a5	success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	Name	unicode	qjrowcce58.exe	success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	Publisher	unicode		success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	Version	unicode		success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	BinFileVersion	unicode		success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	BinaryType	unicode	pe32_i386	success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	ProductName	unicode		success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	ProductVersion	unicode		success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	LinkDate	unicode	04/09/2021 22:57:44	success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	BinProductVersion	unicode		success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	Size	B	00 D8 05 00 00 00 00 00	success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	Language	dword	0	success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	IsPeFile	dword	1	success or wait	1	6FC036BF	unknown
\REGISTRY\A\{4fd15eff-38dc-1bed-78ce-61b9ff404261}\Root\InventoryApplicationFile\qjrowcce58.exe|2dcf57a5	IsOsComponent	dword	0	success or wait	1	6FC036BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 50 83 EC 24 02 00 00 00 08 00 00 00 50 83 EC 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6FC01FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **4412**, Parent PID: **1592**

General

Target ID:	4
Start time:	05:40:15
Start date:	05/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1592 -s 772

Copyright Joe Security LLC 2022

Imagebase:	0x60000
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	6E0F1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAD2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAD2.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_1167fbca	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_1167fbca\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E0E497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAD2.tmp	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAD2.tmp.xml	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE6C7.tmp.csv	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE6D8.tmp.txt	success or wait	1	6E0E497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 73 62 fd 05 12 00 00 00 00 00	MDMP sb	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	6796	6	00 00 00 00 00 00		success or wait	1	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	200	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 1a 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 38 06 00 00 fd fd 73 62 01 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 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	UBGenuineIntelWT8sb0Pacific Standard TimePacific Daylight Time	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	7924	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 fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 50 fd fd 24 1c fd fd 02 00 00 00 00 00 00 40 00 50 fd fd 24 00 00 00 00 28 fd fd 02 50 fd fd 24 23 00 00 00 46 02 01 00 0c fd fd 02 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++P$@P$(P$#F+	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	1620	168	fd 04 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 50 fd fd 24 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 50 fd fd 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 1e 00 00	PP	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	12220	20	35 00 00 00 fd fd 58 00 00 00 00 00 04 00 00 00 10 33 00 00	5X3	success or wait	53	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	13072	4	fd fd 19 00		success or wait	52	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	55172	4	00 00 40 00	@	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	1788	4	05 00 00 00		success or wait	5	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	8640	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 fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 fd 7b 57 77 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 20 fd 19 00 2c fd 4c 77 23 00 00 00 16 02 00 00 00 fd 19 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++{Ww ,Lw#+	success or wait	5	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	1984	48	fd 04 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 2c 00 00 00 00 00 fd fd 02 00 00 00 00 54 12 00 00 fd fd 00 00 fd 02 00 00 fd 2c 00 00	,T,	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	2044	4	26 00 00 00	&	success or wait	38	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	6802	34	1c 00 00 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 00 2e 00 65 00 78 00 65 00 00 00	qjrOWCCE58.exe	success or wait	38	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	6044	752	00 00 fd 6f 00 00 00 00 00 fd 03 00 fd fd 03 00 fd 62 7f fd fd 1e 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 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 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 30 fd 02 00 00 00 00 00 60 02 03 00 00 00 00 37 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 55 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 68 52 1b 00 00 00 00 00 2c 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6d 05 00 00 00 00	obBB?$@AZb0`7hR@m	success or wait	1	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	55176	11008	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF726.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 0c 10 00 00 fd 07 00 00 05 00 00 00 54 03 00 00 fd 2f 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 1d 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 08 18 00 00 16 00 00 00 fd 00 00 00 fd 19 00 00	T/T8T	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 35 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1592</Pid>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 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>qjrOWCCE58.exe</ImageName>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1084	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1182	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 34 00 35 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>9455</Uptime>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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 39 00 35 00 33 00 31 00 38 00 30 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>95318016</PeakVirtualSize>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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 39 00 35 00 33 00 30 00 39 00 38 00 32 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>95309824</VirtualSize>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.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 33 00 30 00 36 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>3065</PageFaultCount>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1696	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 33 00 34 00 35 00 39 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>11345920</PeakWorkingSetSize>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1794	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1798	2	09 00		success or wait	3	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1804	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 33 00 33 00 37 00 37 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>11337728</WorkingSetSize>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1886	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1890	2	09 00		success or wait	3	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	1896	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 37 00 36 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>176984</QuotaPeakPagedPoolUsage>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2010	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2014	2	09 00		success or wait	3	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2020	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 36 00 39 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>176984</QuotaPagedPoolUsage>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2118	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2122	2	09 00		success or wait	3	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2128	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 39 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>37944</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2252	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2256	2	09 00		success or wait	3	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2262	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 35 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>37592</QuotaNonPagedPoolUsage>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2370	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2374	2	09 00		success or wait	3	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2380	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 35 00 39 00 30 00 30 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>2859008</PagefileUsage>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2456	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2460	2	09 00		success or wait	3	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2466	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 32 00 38 00 36 00 37 00 32 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>2867200</PeakPagefileUsage>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2558	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2562	2	09 00		success or wait	3	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2568	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 35 00 39 00 30 00 30 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>2859008</PrivateUsage>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2640	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2644	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2648	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2694	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2698	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2702	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2732	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2736	2	09 00		success or wait	3	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2742	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2782	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2786	2	09 00		success or wait	4	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2794	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2824	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2828	2	09 00		success or wait	4	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2836	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2906	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2910	2	09 00		success or wait	4	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	2918	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3008	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3012	2	09 00		success or wait	4	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3020	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 30 00 32 00 37 00 32 00 39 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6027293</Uptime>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3068	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3072	2	09 00		success or wait	4	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3080	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3158	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3162	2	09 00		success or wait	4	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3170	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3222	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3226	2	09 00		success or wait	4	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3234	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3278	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3282	2	09 00		success or wait	5	6E0E497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3292	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3382	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3386	2	09 00		success or wait	5	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3396	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3470	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3474	2	09 00		success or wait	5	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3484	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 30 00 38 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>46083</PageFaultCount>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3560	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3564	2	09 00		success or wait	5	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3574	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 32 00 33 00 37 00 39 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>102379520</PeakWorkingSetSize>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3674	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3678	2	09 00		success or wait	5	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3688	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 32 00 30 00 31 00 34 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>102014976</WorkingSetSize>	success or wait	1	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3772	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3776	2	09 00		success or wait	5	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3786	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 36 00 37 00 37 00 32 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 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>96772 8</QuotaPeakPagedPoolUsage>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3900	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3904	2	09 00		success or wait	5	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	3914	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 33 00 37 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >937136</Q uotaPagedPoolUsage>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4012	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4016	2	09 00		success or wait	5	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4026	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 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedP oolUsage>70 736</QuotaPeakNonPag edPoolUsage>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4150	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4154	2	09 00		success or wait	5	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4164	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 39 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUs age>69376< /QuotaNonPagedPoolUsa ge>	success or wait	1	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4272	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4276	2	09 00		success or wait	5	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4286	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 38 00 37 00 33 00 33 00 34 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34873344</PagefileUsage>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4364	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4368	2	09 00		success or wait	5	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4378	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 34 00 31 00 38 00 31 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35418112</PeakPagefileUsage>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4472	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4476	2	09 00		success or wait	5	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4486	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 38 00 37 00 33 00 33 00 34 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34873344</PrivateUsage>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4560	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4564	2	09 00		success or wait	4	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4572	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4618	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4622	2	09 00		success or wait	3	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4628	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4670	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4674	2	09 00		success or wait	2	6E0E497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4678	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4716	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4764	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4802	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4806	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4810	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4862	4	0d 00 0a 00		success or wait	9	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4866	2	09 00		success or wait	18	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	4870	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 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>qjrOWCCE58.exe</Parameter0>	success or wait	9	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	5588	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	5592	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	5594	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	5634	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	5638	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	5640	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	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	5678	4	0d 00 0a 00		success or wait	6	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	5682	2	09 00		success or wait	12	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	5686	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6240	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6244	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6246	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6292	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6330	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6334	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6338	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6432	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6436	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6440	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 68 00 6e 00 74 00 71 00 73 00 70 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>hntqsp, Inc.</SystemManufacturer>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6546	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6550	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6554	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 68 00 6e 00 74 00 71 00 73 00 70 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>hntqsp7,1</SystemProductName>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6650	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6654	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6658	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6778	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6782	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6786	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 30 00 34 00 37 00 35 00 37 00 30 00 31 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1604757010</OSInstallDate>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6868	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6872	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6876	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6978	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6982	2	09 00		success or wait	2	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	6986	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7054	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7058	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7060	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7106	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7140	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7144	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7148	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7244	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7248	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7250	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7286	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7290	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7292	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7316	4	0d 00 0a 00		success or wait	3	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7320	2	09 00		success or wait	6	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7324	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 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7582	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7586	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7588	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7614	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7618	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7620	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 30 00 35 00 54 00 31 00 32 00 3a 00 34 00 30 00 3a 00 31 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-05T12:40:16Z">	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7720	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7724	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7728	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 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 35 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 32 00 31 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 32 00 31 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="395" PID="1592" UptimeMS="2218" TimeSinceCreationMS="2218" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7990	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7994	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	7998	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	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8018	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8022	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8024	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8062	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8066	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8068	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8106	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8110	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8114	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 30 00 32 00 63 00 34 00 37 00 33 00 64 00 2d 00 35 00 66 00 38 00 62 00 2d 00 34 00 33 00 32 00 37 00 2d 00 39 00 64 00 64 00 38 00 2d 00 35 00 34 00 39 00 31 00 66 00 34 00 62 00 65 00 66 00 64 00 39 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>002c473d-5f8b-4327-9dd8-5491f4befd91</Guid>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8212	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8216	2	09 00		success or wait	2	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8220	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 30 00 35 00 54 00 31 00 32 00 3a 00 34 00 30 00 3a 00 31 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-05T12:40:16Z</CreationTime>	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8318	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8322	2	09 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8324	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	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8364	4	0d 00 0a 00		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A8.tmp.WERInternalMetadata.xml	8368	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	6E0E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAD2.tmp.xml	0	4704	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_1167fbca\Report.wer	0	2	fd fd		success or wait	1	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_1167fbca\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	163	6E0E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_1167fbca\Report.wer	10688	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 38 00 30 00 32 00 39 00 37 00 39 00 33 00 34 00 35 00	MetadataHash=1802979345	success or wait	1	6E0E497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{66499a53-6730-3b71-8008-baa10338375d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E1036BF	unknown
\REGISTRY\A\{66499a53-6730-3b71-8008-baa10338375d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E1036BF	unknown
\REGISTRY\A\{66499a53-6730-3b71-8008-baa10338375d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0E43D1	unknown

Analysis Process: WerFault.exe PID: **3152**, Parent PID: **1592**

General

Target ID:	8
Start time:	05:40:18
Start date:	05/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1592 -s 796
Imagebase:	0x60000
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	6DF51717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER774.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER774.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_0c0c0928	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_0c0c0928\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER774.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER774.tmp.xml	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF436.tmp.csv	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF447.tmp.txt	success or wait	1	6DF4497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 73 62 fd 05 12 00 00 00 00 00	MDMP sb	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	7108	6	00 00 00 00 00 00		success or wait	1	6DF4497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	200	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 1b 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 38 06 00 00 fd fd 73 62 01 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	UBGenuineIntelWT8sb0Pacific Standard TimePacific Daylight Time	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	8292	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 50 fd fd 24 1c fd fd 02 00 00 00 00 00 00 40 00 50 fd fd 24 00 00 00 00 28 fd fd 02 50 fd fd 24 23 00 00 00 46 02 01 00 0c fd fd 02 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 fd	+S++P$@P$(P$#F+	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	1620	168	74 17 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 50 fd fd 24 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 50 fd fd 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 64 20 00 00	tPPd	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	14020	20	42 00 00 00 fd fd 58 00 00 00 00 00 04 00 00 00 fd 3a 00 00	BX:	success or wait	66	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	15080	4	fd fd 19 00		success or wait	65	6DF4497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	71836	4	00 00 40 00	@	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	1788	4	07 00 00 00		success or wait	7	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	9008	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd 5b 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 19 00 fd fd 4c 77 23 00 00 00 16 02 00 00 60 fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++[Lw#`+	success or wait	7	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	2080	48	fd 08 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 2c 00 00 00 00 00 fd fd fd 02 00 00 00 00 6c 04 00 00 fd 3a 00 00 fd 02 00 00 fd 33 00 00	,l:3	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	2140	4	28 00 00 00	(	success or wait	40	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	7114	34	1c 00 00 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 00 2e 00 65 00 78 00 65 00 00 00	qjrOWCCE58.exe	success or wait	40	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	6356	752	00 00 fd 6a 00 00 00 00 00 50 22 00 43 6f 22 00 fd 72 23 46 20 00 00 fd 04 fd fd 00 00 01 00 00 00 0b 00 01 00 fd 42 00 00 0b 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 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 60 fd 02 00 00 00 00 00 60 02 03 00 00 00 00 3e 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 21 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 36 1b 00 00 00 00 00 67 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6d 05 00 00 00 00	jP"Co"r#F BB? %@AZb``>!6g@m	success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	71840	11912	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38A.tmp.dmp	32	108	03 00 00 00 54 01 00 00 fd 06 00 00 04 00 00 00 fd 10 00 00 5c 08 00 00 05 00 00 00 24 04 00 00 fd 36 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 20 00 00 48 26 01 00 15 00 00 00 fd 01 00 00 40 19 00 00 16 00 00 00 fd 00 00 00 2c 1b 00 00	T\$6T8T H&@,	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 35 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1592</Pid>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 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>qjrOWCCE58.exe</ImageName>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1084	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1182	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 36 00 37 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>12673</Uptime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1226	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1230	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1234	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1316	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1320	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1324	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1376	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1380	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1384	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1428	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1432	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1438	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 38 00 38 00 38 00 30 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>101888000</PeakVirtualSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1536	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 38 00 37 00 39 00 38 00 30 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>101879808</VirtualSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1608	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1612	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1618	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 34 00 34 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>3443</PageFaultCount>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1692	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1696	2	09 00		success or wait	3	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1702	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 35 00 36 00 36 00 35 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>12566528</PeakWorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1800	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1804	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1810	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 35 00 36 00 36 00 35 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>12566528</WorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1892	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1896	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	1902	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 38 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>184872</QuotaPeakPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2016	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2020	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2026	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 38 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>184856</QuotaPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2124	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2128	2	09 00		success or wait	3	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2134	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 38 00 32 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>46824</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2258	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2262	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2268	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 34 00 37 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>46472</QuotaNonPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2376	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2380	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2386	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 33 00 31 00 37 00 34 00 34 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3174400</PagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2462	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2466	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2472	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 38 00 32 00 35 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>31825 92</PeakPagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2564	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2568	2	09 00		success or wait	3	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2574	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 33 00 31 00 37 00 34 00 34 00 30 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3174400</PrivateUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2646	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2650	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2654	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2700	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2704	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2708	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2738	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2742	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2748	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2788	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2792	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2800	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2830	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2834	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2842	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2912	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2916	2	09 00		success or wait	4	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	2924	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3014	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3018	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3026	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 30 00 33 00 30 00 34 00 36 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6030464</Uptime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3086	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3176	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3240	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	6DF4497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3298	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3388	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3392	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3402	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3476	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3480	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3490	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 30 00 38 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>46085</PageFaultCount>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3566	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3570	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3580	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 32 00 33 00 37 00 39 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>102379520</PeakWorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3680	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3684	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3694	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 31 00 39 00 39 00 30 00 34 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>101990400</WorkingSetSize>	success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3778	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3782	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3792	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 36 00 37 00 37 00 32 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 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>96772 8</QuotaPeakPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3906	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3910	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	3920	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 33 00 37 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >937136</Q uotaPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4018	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4022	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4032	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedP oolUsage>70 736</QuotaPeakNonPag edPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4156	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4160	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4170	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 39 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUs age>69376< /QuotaNonPagedPoolUsa ge>	success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4278	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4282	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4292	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 38 00 37 00 33 00 33 00 34 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34873344</PagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4370	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4374	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4384	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 34 00 31 00 38 00 31 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35418112</PeakPagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4478	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4482	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4492	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 38 00 37 00 33 00 33 00 34 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34873344</PrivateUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4566	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4570	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4578	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4624	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4628	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4634	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4676	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4680	2	09 00		success or wait	2	6DF4497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4684	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4716	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4720	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4722	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4764	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4768	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4770	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4808	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4812	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4816	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4868	4	0d 00 0a 00		success or wait	9	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4872	2	09 00		success or wait	18	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	4876	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 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>qjrOWCCE58.exe</Parameter0>	success or wait	9	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	5594	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	5598	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	5600	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	5640	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	5644	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	5646	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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	5684	4	0d 00 0a 00		success or wait	6	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	5688	2	09 00		success or wait	12	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	5692	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6246	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6250	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6252	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6292	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6296	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6298	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6336	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6340	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6344	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6438	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6442	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6446	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 68 00 6e 00 74 00 71 00 73 00 70 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>hntqsp, Inc.</SystemManufacturer>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6552	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6556	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6560	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 68 00 6e 00 74 00 71 00 73 00 70 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>hntqsp7,1</SystemProductName>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6656	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6660	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6664	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6784	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6788	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6792	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 30 00 34 00 37 00 35 00 37 00 30 00 31 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1604757010</OSInstallDate>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6874	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6878	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6882	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6984	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6988	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	6992	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7060	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7064	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7066	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7106	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7110	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7112	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7146	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7150	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7154	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7250	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7254	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7256	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7292	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7296	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7298	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7322	4	0d 00 0a 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7326	2	09 00		success or wait	6	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7330	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 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7588	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7592	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7594	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7620	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7624	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7626	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 30 00 35 00 54 00 31 00 32 00 3a 00 34 00 30 00 3a 00 31 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-05T12:40:19Z">	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7726	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7730	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7734	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 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 35 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 32 00 31 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 32 00 31 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="395" PID="1592" UptimeMS="2218" TimeSinceCreationMS="2218" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	7996	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8000	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8004	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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8024	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8028	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8030	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8068	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8072	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8074	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8112	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8116	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8120	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 34 00 32 00 64 00 66 00 38 00 64 00 30 00 2d 00 62 00 33 00 31 00 36 00 2d 00 34 00 37 00 39 00 34 00 2d 00 38 00 62 00 64 00 30 00 2d 00 34 00 32 00 36 00 61 00 65 00 34 00 65 00 31 00 32 00 38 00 61 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>a42df8d0-b316-4794-8bd0-426ae4e128a6</Guid>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8218	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8222	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8226	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 30 00 35 00 54 00 31 00 32 00 3a 00 34 00 30 00 3a 00 31 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-05T12:40:19Z</CreationTime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8324	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8328	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8330	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8370	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63B.tmp.WERInternalMetadata.xml	8374	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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER774.tmp.xml	0	4704	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_0c0c0928\Report.wer	0	2	fd fd		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_0c0c0928\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	165	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_0c0c0928\Report.wer	10888	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 30 00 34 00 35 00 36 00 33 00 37 00 37 00 33 00 32 00	MetadataHash=-1045637732	success or wait	1	6DF4497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{334b5f79-f960-037b-181d-14ae1ad026fd}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF636BF	unknown
\REGISTRY\A\{334b5f79-f960-037b-181d-14ae1ad026fd}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF636BF	unknown
\REGISTRY\A\{334b5f79-f960-037b-181d-14ae1ad026fd}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF443D1	unknown

Analysis Process: WerFault.exe PID: **4228**, Parent PID: **1592**

General

Target ID:	11
Start time:	05:40:25
Start date:	05/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1592 -s 628
Imagebase:	0x60000
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	6DF51717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER21C3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER21C3.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_10d822ca	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_10d822ca\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER21C3.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER21C3.tmp.xml	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0A.tmp.csv	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1A.tmp.txt	success or wait	1	6DF4497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 73 62 fd 05 12 00 00 00 00 00	MDMP sb	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	7108	6	00 00 00 00 00 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	200	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 1b 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 38 06 00 00 fd fd 73 62 01 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 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	UBGenuineIntelWT8sb0Pacific Standard TimePacific Daylight Time	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	8292	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 50 fd fd 24 1c fd fd 02 00 00 00 00 00 00 40 00 50 fd fd 24 00 00 00 00 28 fd fd 02 50 fd fd 24 23 00 00 00 46 02 01 00 0c fd fd 02 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 fd	+S++P$@P$(P$#F+	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	1620	168	fd 08 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 50 fd fd 24 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 50 fd fd 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 64 20 00 00	PPd	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	14020	20	42 00 00 00 fd fd 02 00 00 00 00 54 12 00 00 fd 3a 00 00	BT:	success or wait	66	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	15080	4692	fd fd 4c 77 fd 1d 51 77 fd fd fd fd fd fd 02 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 38 fd 02 00 00 00 00 0c 03 00 00 00 00 00 00 00 00 00 00 0c 03 00 00 fd 02 00 00 78 fd 02 fd fd fd fd 78 fd 02 12 12 51 77 fd 02 00 00 00 00 00 00 fd fd fd fd fd fd 02 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 6c fd 02 1c fd 02 fd 02 00 00 00 00 fd 00 04 00 00 00 74 02 00 00 60 03 00 00 24 03 00 00 0c 03 00 00 00 00 00 00 0c 03 00 00 74 02 00 00 24 03 00 00 60 03 00 00 fd fd fd fd 00 fd 02 fd fd fd fd 2c fd 02 fd 17 4d 77 fd fd fd fd 00 00 00 00 fd fd 02 fd 0c 51 77 fd fd fd fd 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd 02 3d fd 50 77 1c fd 02 6c fd 02 fd fd fd fd 00 00 00	LwQw8xxQwlt`$t$`,MwQw=Pwl	success or wait	65	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	71024	4	00 00 40 00	@	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	1788	4	07 00 00 00		success or wait	7	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	9008	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 5b 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 19 00 fd fd 4c 77 23 00 00 00 16 02 00 00 60 fd 19 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++[Lw#`+	success or wait	7	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	2080	48	fd 08 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 2c 00 00 00 00 00 fd fd 02 00 00 00 00 54 12 00 00 fd 3a 00 00 fd 02 00 00 fd 33 00 00	,T:3	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	2140	4	28 00 00 00	(	success or wait	40	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	7114	34	1c 00 00 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 00 2e 00 65 00 78 00 65 00 00 00	qjrOWCCE58.exe	success or wait	40	6DF4497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	6356	752	00 00 fd 6a 00 00 00 00 00 50 22 00 43 6f 22 00 fd 72 23 46 20 00 00 fd 04 fd fd 00 00 01 00 00 00 0b 00 01 00 fd 42 00 00 0b 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 25 00 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 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 00 60 02 03 00 00 00 00 38 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 6b fd 03 00 00 00 00 00 21 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 18 28 1b 00 00 00 00 00 28 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6d 05 00 00 00 00	jP"Co"r#F BB? %@AZb`8k!((@m	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	71028	11912	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1DD9.tmp.dmp	32	108	03 00 00 00 54 01 00 00 fd 06 00 00 04 00 00 00 fd 10 00 00 5c 08 00 00 05 00 00 00 24 04 00 00 fd 36 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 20 00 00 1c 23 01 00 15 00 00 00 fd 01 00 00 40 19 00 00 16 00 00 00 fd 00 00 00 2c 1b 00 00	T\$6T8T #@,	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 35 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1592</Pid>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 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>qjrOWCCE58.exe</ImageName>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1084	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>000000000</CmdLineSignature>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1182	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 34 00 39 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>19495</Uptime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1226	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1230	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1234	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1316	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1320	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1324	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1376	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1380	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1384	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1428	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1432	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1438	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 38 00 38 00 38 00 30 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>101888000</PeakVirtualSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1536	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 38 00 37 00 39 00 38 00 30 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>101879808</VirtualSize>	success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1608	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1612	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1618	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 35 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>3517</PageFaultCount>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1692	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1696	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1702	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 35 00 38 00 32 00 39 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>12582912</PeakWorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1800	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1804	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1810	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 35 00 37 00 30 00 36 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>12570624</WorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1892	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1896	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	1902	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 38 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>184872</QuotaPeakPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2016	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2020	2	09 00		success or wait	3	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2026	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 38 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>184856</QuotaPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2124	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2128	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2134	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 35 00 31 00 30 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 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>51016</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2258	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2262	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2268	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 35 00 30 00 36 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>50664</QuotaNonPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2376	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2380	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2386	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 33 00 31 00 37 00 38 00 34 00 39 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>3178496</PagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2462	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2466	2	09 00		success or wait	3	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2472	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 38 00 36 00 36 00 38 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>3186688</PeakPagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2564	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2568	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2574	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 33 00 31 00 37 00 38 00 34 00 39 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>3178496</PrivateUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2646	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2650	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2654	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2700	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2704	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2708	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2738	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2742	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2748	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2788	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2792	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2800	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2830	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2834	2	09 00		success or wait	4	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2842	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2912	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2916	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	2924	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3014	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3018	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3026	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 30 00 33 00 37 00 33 00 33 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6037332</Uptime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3086	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3176	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3240	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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3298	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3388	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3392	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3402	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3476	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3480	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3490	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 37 00 30 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>46704</PageFaultCount>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3566	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3570	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3580	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 32 00 33 00 37 00 39 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>102379520</PeakWorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3680	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3684	2	09 00		success or wait	5	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3694	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 36 00 33 00 32 00 38 00 33 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>96632832</WorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3776	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3780	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3790	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 36 00 37 00 37 00 32 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 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>967728</QuotaPeakPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3904	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3908	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	3918	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 38 00 34 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>928464</QuotaPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4016	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4020	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4030	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 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>70736</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4154	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4158	2	09 00		success or wait	5	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4168	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 36 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>68696</QuotaNonPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4276	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4280	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4290	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 33 00 31 00 30 00 39 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>293109776</PagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4368	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4372	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4382	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 34 00 31 00 38 00 31 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35418112</PeakPagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4476	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4480	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4490	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 33 00 31 00 30 00 39 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>29310976</PrivateUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4564	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4568	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4576	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4632	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4674	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4678	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4682	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4720	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4762	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4766	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4768	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4806	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4810	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4814	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	9	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	18	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	4874	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 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>qjrOWCCE58.exe</Parameter0>	success or wait	9	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	5592	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	5596	2	09 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	5598	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	5638	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	5642	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	5644	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	5682	4	0d 00 0a 00		success or wait	6	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	5686	2	09 00		success or wait	12	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	5690	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6244	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6248	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6250	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6290	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6294	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6296	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6334	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6338	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6342	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6436	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6440	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6444	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 68 00 6e 00 74 00 71 00 73 00 70 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>hntqsp, Inc.</SystemManufacturer>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6550	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6554	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6558	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 68 00 6e 00 74 00 71 00 73 00 70 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>hntqsp7,1</SystemProductName>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6654	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6658	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6662	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6782	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6786	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6790	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 30 00 34 00 37 00 35 00 37 00 30 00 31 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1604757010</OSInstallDate>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6872	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6876	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6880	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6982	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6986	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	6990	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7058	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7062	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7064	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7104	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7108	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7110	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7144	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7148	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7152	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7248	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7252	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7254	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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7290	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7294	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7296	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7320	4	0d 00 0a 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7324	2	09 00		success or wait	6	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7328	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 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7586	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7590	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7592	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7618	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7622	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7624	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 30 00 35 00 54 00 31 00 32 00 3a 00 34 00 30 00 3a 00 32 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-05T12:40:26Z">	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7724	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7728	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7732	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 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 35 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 32 00 31 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 32 00 31 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="395" PID="1592" UptimeMS="2218" TimeSinceCreationMS="2218" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7994	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	7998	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8002	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8022	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8026	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8028	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8066	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8070	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8072	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8110	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8114	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8118	98	3c 00 47 00 75 00 69 00 64 00 3e 00 34 00 36 00 38 00 63 00 31 00 37 00 61 00 66 00 2d 00 63 00 34 00 38 00 38 00 2d 00 34 00 62 00 64 00 35 00 2d 00 61 00 30 00 31 00 32 00 2d 00 64 00 32 00 38 00 36 00 64 00 33 00 66 00 38 00 33 00 30 00 34 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>468c17af-c488-4bd5-a012-d286d3f83040</Guid>	success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8216	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8220	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8224	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 30 00 35 00 54 00 31 00 32 00 3a 00 34 00 30 00 3a 00 32 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>2022-05-05T12:40:26Z</CreationTime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8322	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8326	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8328	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8368	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20D7.tmp.WERInternalMetadata.xml	8372	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER21C3.tmp.xml	0	4704	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_10d822ca\Report.wer	0	2	fd fd		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_10d822ca\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	165	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_10d822ca\Report.wer	10890	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 30 00 31 00 39 00 39 00 39 00 35 00 37 00 39 00 37 00	MetadataHash=1019995797	success or wait	1	6DF4497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{30ea652d-2dbe-0c05-2fbf-c2a2139ac408}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF636BF	unknown
\REGISTRY\A\{30ea652d-2dbe-0c05-2fbf-c2a2139ac408}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF636BF	unknown
\REGISTRY\A\{30ea652d-2dbe-0c05-2fbf-c2a2139ac408}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF443D1	unknown

Analysis Process: WerFault.exe PID: **4856**, Parent PID: **1592**

General

Target ID:	15
Start time:	05:40:28
Start date:	05/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1592 -s 900
Imagebase:	0x60000
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	6DF51717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER329B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER329B.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_12a4344f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_12a4344f\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER329B.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER329B.tmp.xml	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F52.tmp.csv	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F82.tmp.txt	success or wait	1	6DF4497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 73 62 fd 05 12 00 00 00 00 00	MDMP sb	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	7252	6	00 00 00 00 00 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	200	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 54 1c 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 38 06 00 00 fd fd 73 62 01 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 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00	UBTGenuineIntelWT8sb0Pacific Standard TimePacific Daylight Time	success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	8436	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 50 fd fd 24 1c fd fd 02 00 00 00 00 00 00 40 00 50 fd fd 24 00 00 00 00 28 fd fd 02 50 fd fd 24 23 00 00 00 46 02 01 00 0c fd fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++P$@P$(P$#F+	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	1620	168	fd 05 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 50 fd fd 24 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 50 fd fd 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 20 00 00	PP	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	16312	20	42 00 00 00 fd fd 58 00 00 00 00 00 04 00 00 00 fd 43 00 00	BXC	success or wait	66	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	17372	4	fd fd 19 00		success or wait	65	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	83256	4	00 00 40 00	@	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	1788	4	0a 00 00 00		success or wait	10	6DF4497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	9152	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 64 03 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 2c fd 4c 77 23 00 00 00 06 02 00 00 fd fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++d ,Lw#+	success or wait	10	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	2224	48	54 04 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 70 2d 00 00 00 00 00 fd fd fd 02 00 00 00 00 6c 04 00 00 fd 46 00 00 fd 02 00 00 fd 3c 00 00	T p-lF<	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	2284	4	28 00 00 00	(	success or wait	40	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	7258	34	1c 00 00 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 00 2e 00 65 00 78 00 65 00 00 00	qjrOWCCE58.exe	success or wait	40	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	6500	752	00 00 fd 6a 00 00 00 00 00 50 22 00 43 6f 22 00 fd 72 23 fd 20 00 00 fd 04 fd fd 00 00 01 00 00 00 0b 00 01 00 fd 42 00 00 0b 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 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 30 fd 02 00 00 00 00 00 60 02 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 3c fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 44 0b 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6d 05 00 00 00 00	jP"Co"r# BB? %@AZb0`<D@m	success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	83260	12494	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2CBD.tmp.dmp	32	108	03 00 00 00 fd 01 00 00 fd 06 00 00 04 00 00 00 fd 10 00 00 fd 08 00 00 05 00 00 00 24 04 00 00 fd 3f 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 20 22 00 00 fd 53 01 00 15 00 00 00 fd 01 00 00 fd 19 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	$?T8T "S	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 35 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1592</Pid>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 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>qjrOWCCE58.exe</ImageName>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1084	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1182	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 33 00 35 00 38 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>23586</Uptime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1226	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1230	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1234	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1316	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1320	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1324	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1376	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1380	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1384	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1428	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1432	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1438	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 38 00 32 00 30 00 31 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>105820160</PeakVirtualSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1536	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 38 00 31 00 31 00 39 00 36 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>105811968</VirtualSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1608	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1612	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1618	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 36 00 37 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>3679</PageFaultCount>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1692	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1696	2	09 00		success or wait	3	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1702	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 31 00 36 00 33 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>12816384</PeakWorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1800	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1804	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1810	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 30 00 34 00 30 00 39 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>12804096</WorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1892	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1896	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	1902	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 35 00 30 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>185024</QuotaPeakPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2016	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2020	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2026	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 38 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>184856</QuotaPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2124	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2128	2	09 00		success or wait	3	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2134	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 35 00 38 00 32 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>58200</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2258	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2262	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2268	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 35 00 37 00 38 00 34 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>57848</QuotaNonPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2376	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2380	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2386	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 33 00 34 00 32 00 38 00 33 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3428352</PagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2462	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2466	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2472	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 33 00 36 00 35 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3436544</PeakPagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2564	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2568	2	09 00		success or wait	3	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2574	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 33 00 34 00 32 00 38 00 33 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3428352</PrivateUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2646	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2650	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2654	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2700	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2704	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2708	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2738	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2742	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2748	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2788	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2792	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2800	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2830	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2834	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2842	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2912	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2916	2	09 00		success or wait	4	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	2924	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3014	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3018	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3026	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 30 00 34 00 31 00 33 00 37 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6041377</Uptime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3086	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3176	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3240	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	6DF4497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3298	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3388	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3392	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3402	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3476	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3480	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3490	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 38 00 32 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>48276</PageFaultCount>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3566	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3570	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3580	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 32 00 33 00 37 00 39 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>102379520</PeakWorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3680	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3684	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3694	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 31 00 39 00 39 00 34 00 34 00 39 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>101994496</WorkingSetSize>	success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3778	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3782	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3792	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 36 00 37 00 37 00 32 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 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>967728</QuotaPeakPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3906	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3910	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	3920	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 31 00 38 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>921808</QuotaPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4018	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4022	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4032	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>70736</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4156	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4160	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4170	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4278	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4282	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4292	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 34 00 32 00 35 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34242560</PagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4370	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4374	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4384	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 34 00 31 00 38 00 31 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35418112</PeakPagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4478	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4482	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4492	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 34 00 32 00 35 00 36 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34242560</PrivateUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4566	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4570	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4578	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4624	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4628	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4634	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4676	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4680	2	09 00		success or wait	2	6DF4497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4684	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4716	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4720	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4722	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4764	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4768	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4770	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4808	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4812	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4816	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4868	4	0d 00 0a 00		success or wait	9	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4872	2	09 00		success or wait	18	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	4876	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 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>qjrOWCCE58.exe</Parameter0>	success or wait	9	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	5594	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	5598	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	5600	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	5640	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	5644	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	5646	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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	5684	4	0d 00 0a 00		success or wait	6	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	5688	2	09 00		success or wait	12	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	5692	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6246	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6250	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6252	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6292	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6296	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6298	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6336	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6340	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6344	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6438	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6442	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6446	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 68 00 6e 00 74 00 71 00 73 00 70 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>hntqsp, Inc.</SystemManufacturer>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6552	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6556	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6560	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 68 00 6e 00 74 00 71 00 73 00 70 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>hntqsp7,1</SystemProductName>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6656	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6660	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6664	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6784	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6788	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6792	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 30 00 34 00 37 00 35 00 37 00 30 00 31 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1604757010</OSInstallDate>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6874	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6878	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6882	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6984	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6988	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	6992	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7060	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7064	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7066	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7106	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7110	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7112	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7146	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7150	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7154	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</UEFI SecureBootEnabled>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7250	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7254	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7256	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7292	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7296	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7298	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7322	4	0d 00 0a 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7326	2	09 00		success or wait	6	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7330	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 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7588	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7592	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7594	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7620	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7624	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7626	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 30 00 35 00 54 00 31 00 32 00 3a 00 34 00 30 00 3a 00 33 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-05T12:40:30Z">	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7726	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7730	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7734	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 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 35 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 32 00 31 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 32 00 31 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="395" PID="1592" UptimeMS="2218" TimeSinceCreationMS="2218" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	7996	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8000	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8004	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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8024	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8028	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8030	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8068	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8072	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8074	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8112	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8116	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8120	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 61 00 64 00 36 00 37 00 66 00 62 00 37 00 2d 00 32 00 64 00 32 00 33 00 2d 00 34 00 66 00 61 00 35 00 2d 00 39 00 36 00 62 00 63 00 2d 00 39 00 34 00 63 00 37 00 32 00 66 00 64 00 32 00 35 00 66 00 65 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>7ad67fb7-2d23-4fa5-96bc-94c72fd25fee</Guid>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8218	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8222	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8226	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 30 00 35 00 54 00 31 00 32 00 3a 00 34 00 30 00 3a 00 33 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>2022-05-05T12:40:30Z</CreationTime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8324	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8328	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8330	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8370	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30D5.tmp.WERInternalMetadata.xml	8374	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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER329B.tmp.xml	0	4704	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_12a4344f\Report.wer	0	2	fd fd		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_12a4344f\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	165	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_12a4344f\Report.wer	10890	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 38 00 33 00 38 00 30 00 32 00 32 00 34 00 34 00 34 00	MetadataHash=1838022444	success or wait	1	6DF4497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{fce02c4a-13c0-40af-9c5c-bf3efbb2f3b1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF636BF	unknown
\REGISTRY\A\{fce02c4a-13c0-40af-9c5c-bf3efbb2f3b1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF636BF	unknown
\REGISTRY\A\{fce02c4a-13c0-40af-9c5c-bf3efbb2f3b1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF443D1	unknown

Analysis Process: WerFault.exe PID: **6220**, Parent PID: **1592**

General

Target ID:	22
Start time:	05:40:33
Start date:	05/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1592 -s 908
Imagebase:	0x60000
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	6DF51717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4306.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4306.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_181043fe	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_181043fe\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4306.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4306.tmp.xml	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F23.tmp.csv	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F33.tmp.txt	success or wait	1	6DF4497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 73 62 fd 05 12 00 00 00 00 00	MDMP sb	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	7252	6	00 00 00 00 00 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	200	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 54 1c 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 38 06 00 00 fd fd 73 62 01 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	UBTGenuineIntelWT8sb0 Pacific Standard TimePacific Daylight T ime	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	8436	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 50 fd fd 24 1c fd fd 02 00 00 00 00 00 00 40 00 50 fd fd 24 00 00 00 00 28 fd fd 02 50 fd fd 24 23 00 00 00 46 02 01 00 0c fd fd 02 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++P$@P$(P$#F+	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	1620	168	50 0c 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 50 fd fd 24 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 50 fd fd 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 20 00 00	PPP	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	16312	20	44 00 00 00 fd fd 58 00 00 00 00 00 04 00 00 00 fd 43 00 00	DXC	success or wait	68	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	17404	4	fd fd 19 00		success or wait	67	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	82736	4	00 00 40 00	@	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	1788	4	0a 00 00 00		success or wait	10	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	9152	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 64 03 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 2c fd 4c 77 23 00 00 00 06 02 00 00 fd fd 19 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++d ,Lw#+	success or wait	10	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	2224	48	54 04 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 70 2d 00 00 00 00 00 fd fd fd 02 00 00 00 00 6c 04 00 00 fd 46 00 00 fd 02 00 00 fd 3c 00 00	T p-lF<	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	2284	4	28 00 00 00	(	success or wait	40	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	7258	34	1c 00 00 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 00 2e 00 65 00 78 00 65 00 00 00	qjrOWCCE58.exe	success or wait	40	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	6500	752	00 00 fd 6a 00 00 00 00 00 50 22 00 43 6f 22 00 fd 72 23 fd 20 00 00 fd 04 fd fd 00 00 01 00 00 00 0b 00 01 00 fd 42 00 00 0b 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 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 20 fd 02 00 00 00 00 00 60 02 03 00 00 00 00 37 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 1c 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6d 05 00 00 00 00	jP"Co"r# BB?%@AZb `7@m	success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	82740	12494	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3EED.tmp.dmp	32	108	03 00 00 00 fd 01 00 00 fd 06 00 00 04 00 00 00 fd 10 00 00 fd 08 00 00 05 00 00 00 44 04 00 00 fd 3f 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 20 22 00 00 fd 51 01 00 15 00 00 00 fd 01 00 00 fd 19 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	D?T8T "Q	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 35 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1592</Pid>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 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>qjrOWCCE58.exe</ImageName>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1084	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1182	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 37 00 39 00 34 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>27942</Uptime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1226	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1230	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1234	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1316	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1320	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1324	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1376	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1380	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1384	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1428	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1432	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1438	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 38 00 32 00 30 00 31 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>105820160</PeakVirtualSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1536	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 38 00 31 00 31 00 39 00 36 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>105811968</VirtualSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1608	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1612	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1618	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 37 00 38 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>3783</PageFaultCount>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1692	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1696	2	09 00		success or wait	3	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1702	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 32 00 30 00 34 00 38 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>12820480</PeakWorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1800	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1804	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1810	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 30 00 38 00 31 00 39 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>12808192</WorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1892	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1896	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	1902	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 35 00 30 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>185024</QuotaPeakPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2016	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2020	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2026	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 38 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>184856</QuotaPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2124	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2128	2	09 00		success or wait	3	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2134	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 36 00 32 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>62744</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2258	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2262	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2268	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 32 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>62392</QuotaNonPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2376	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2380	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2386	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 33 00 34 00 33 00 32 00 34 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3432448</PagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2462	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2466	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2472	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 34 00 30 00 36 00 34 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>3440640</PeakPagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2564	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2568	2	09 00		success or wait	3	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2574	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 33 00 34 00 33 00 32 00 34 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3432448</PrivateUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2646	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2650	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2654	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2700	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2704	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2708	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2738	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2742	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2748	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2788	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2792	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2800	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2830	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2834	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2842	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2912	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2916	2	09 00		success or wait	4	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	2924	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3014	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3018	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3026	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 30 00 34 00 35 00 37 00 33 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6045733</Uptime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3086	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3176	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3240	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	6DF4497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3298	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3388	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3392	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3402	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3476	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3480	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3490	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 38 00 33 00 30 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>48301</PageFaultCount>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3566	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3570	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3580	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 32 00 33 00 37 00 39 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>102379520</PeakWorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3680	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3684	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3694	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 37 00 39 00 36 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>9679672</WorkingSetSize>	success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3776	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3780	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3790	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 36 00 37 00 37 00 32 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 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>96772 8</QuotaPeakPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3904	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3908	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	3918	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 31 00 38 00 33 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 >921832</Q uotaPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4016	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4020	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4030	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 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedP oolUsage>70 736</QuotaPeakNonPag edPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4154	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4158	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4168	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 35 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUs age>68560< /QuotaNonPagedPoolUsa ge>	success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4276	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4280	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4290	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 30 00 30 00 37 00 38 00 37 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>290078 72</PagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4368	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4372	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4382	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 34 00 31 00 38 00 31 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35 418112</P eakPagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4476	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4480	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4490	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 30 00 30 00 37 00 38 00 37 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>2900787 2</PrivateUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4564	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4568	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4576	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4632	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4674	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4678	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4682	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4720	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4762	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4766	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4768	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4806	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4810	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4814	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	9	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	18	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	4874	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 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>qjrOWCCE58.exe</Parameter0>	success or wait	9	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	5592	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	5596	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	5598	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	5638	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	5642	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	5644	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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	5682	4	0d 00 0a 00		success or wait	6	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	5686	2	09 00		success or wait	12	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	5690	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6244	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6248	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6250	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6290	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6294	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6296	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6334	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6338	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6342	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6436	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6440	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6444	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 68 00 6e 00 74 00 71 00 73 00 70 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>hntqsp, Inc.</SystemManufacturer>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6550	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6554	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6558	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 68 00 6e 00 74 00 71 00 73 00 70 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>hntqsp7,1</SystemProductName>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6654	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6658	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6662	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6782	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6786	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6790	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 30 00 34 00 37 00 35 00 37 00 30 00 31 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1604757010</OSInstallDate>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6872	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6876	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6880	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6982	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6986	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	6990	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7058	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7062	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7064	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7104	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7108	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7110	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7144	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7148	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7152	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7248	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7252	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7254	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7290	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7294	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7296	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7320	4	0d 00 0a 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7324	2	09 00		success or wait	6	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7328	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 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7586	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7590	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7592	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7618	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7622	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7624	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 30 00 35 00 54 00 31 00 32 00 3a 00 34 00 30 00 3a 00 33 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-05T12:40:34Z">	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7724	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7728	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7732	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 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 35 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 32 00 31 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 32 00 31 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="395" PID="1592" UptimeMS="2218" TimeSinceCreationMS="2218" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7994	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	7998	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8002	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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8022	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8026	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8028	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8066	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8070	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8072	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8110	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8114	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8118	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 61 00 32 00 61 00 61 00 64 00 36 00 32 00 2d 00 33 00 61 00 39 00 38 00 2d 00 34 00 33 00 31 00 66 00 2d 00 62 00 66 00 64 00 36 00 2d 00 32 00 34 00 39 00 64 00 39 00 30 00 38 00 63 00 35 00 64 00 61 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>1a2aad62-3a98-431f-bfd6-249d908c5da0</Guid>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8216	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8220	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8224	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 30 00 35 00 54 00 31 00 32 00 3a 00 34 00 30 00 3a 00 33 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-05T12:40:34Z</CreationTime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8322	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8326	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8328	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8368	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER41DC.tmp.WERInternalMetadata.xml	8372	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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4306.tmp.xml	0	4704	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_181043fe\Report.wer	0	2	fd fd		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_181043fe\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	165	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_181043fe\Report.wer	10890	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 38 00 30 00 38 00 38 00 33 00 31 00 30 00 38 00 37 00	MetadataHash=-808831087	success or wait	1	6DF4497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{99044a5e-c95f-82c3-9b7e-191f2d2e7a73}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF636BF	unknown
\REGISTRY\A\{99044a5e-c95f-82c3-9b7e-191f2d2e7a73}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF636BF	unknown
\REGISTRY\A\{99044a5e-c95f-82c3-9b7e-191f2d2e7a73}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF443D1	unknown

Analysis Process: WerFault.exe PID: **6408**, Parent PID: **1592**

General

Target ID:	25
Start time:	05:40:36
Start date:	05/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1592 -s 916
Imagebase:	0x60000
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	6DF51717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER51AC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER51AC.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_19545302	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_19545302\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER51AC.tmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER51AC.tmp.xml	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3E19.tmp.csv	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3E39.tmp.txt	success or wait	1	6DF4497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 73 62 fd 05 12 00 00 00 00 00	MDMP sb	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	7252	6	00 00 00 00 00 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	200	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 54 1c 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 38 06 00 00 fd fd 73 62 01 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 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	UBTGenuineIntelWT8sb0 Pacific Standard TimePacific Daylight T ime	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	8436	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 50 fd fd 24 1c fd fd 02 00 00 00 00 00 00 40 00 50 fd fd 24 00 00 00 00 28 fd fd 02 50 fd fd 24 23 00 00 00 46 02 01 00 0c fd fd 02 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 fd fd	+S++P$@P$(P$#F+	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	1620	168	54 04 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 50 fd fd 24 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 50 fd fd 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 20 00 00	TPP	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	16312	20	44 00 00 00 fd fd 58 00 00 00 00 00 04 00 00 00 fd 43 00 00	DXC	success or wait	68	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	17404	4	fd fd 19 00		success or wait	67	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	82560	4	00 00 40 00	@	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	1788	4	0a 00 00 00		success or wait	10	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	9152	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 fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 64 03 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 2c fd 4c 77 23 00 00 00 06 02 00 00 fd fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++d ,Lw#+	success or wait	10	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	2224	48	54 04 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 70 2d 00 00 00 00 00 fd fd fd 02 00 00 00 00 54 12 00 00 fd 46 00 00 fd 02 00 00 fd 3c 00 00	T p-TF<	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	2284	4	28 00 00 00	(	success or wait	40	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	7258	34	1c 00 00 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 00 2e 00 65 00 78 00 65 00 00 00	qjrOWCCE58.exe	success or wait	40	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	6500	752	00 00 fd 6a 00 00 00 00 00 50 22 00 43 6f 22 00 fd 72 23 fd 20 00 00 fd 04 fd fd 00 00 01 00 00 00 0b 00 01 00 fd 42 00 00 0b 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 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 60 fd 02 00 00 00 00 00 60 02 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 d5 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 11 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6d 05 00 00 00 00	jP"Co"r# BB? %@AZb``@m	success or wait	1	6DF4497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	82564	12702	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C2C.tmp.dmp	32	108	03 00 00 00 fd 01 00 00 fd 06 00 00 04 00 00 00 fd 10 00 00 fd 08 00 00 05 00 00 00 44 04 00 00 fd 3f 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 22 00 00 fd 51 01 00 15 00 00 00 fd 01 00 00 fd 19 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	D?T8T"Q	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 35 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1592</Pid>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 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>qjrOWCCE58.exe</ImageName>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1084	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1182	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 31 00 35 00 39 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>31590</Uptime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1226	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1230	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1234	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1316	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1320	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1324	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1376	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1380	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1384	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1428	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1432	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1438	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 38 00 32 00 30 00 31 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>105820160</PeakVirtualSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1536	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 38 00 31 00 31 00 39 00 36 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>105811968</VirtualSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1608	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1612	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1618	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 38 00 38 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>3888</PageFaultCount>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1692	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1696	2	09 00		success or wait	3	6DF4497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1702	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 32 00 38 00 36 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>12828672</PeakWorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1800	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1804	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1810	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 31 00 36 00 33 00 38 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>12816384</WorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1892	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1896	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	1902	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 35 00 30 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>185024</QuotaPeakPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2016	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2020	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2026	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 38 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>184856</QuotaPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2124	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2128	2	09 00		success or wait	3	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2134	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 36 00 36 00 39 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>66904</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2258	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2262	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2268	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 36 00 35 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>66552</QuotaNonPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2376	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2380	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2386	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 33 00 34 00 34 00 30 00 36 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3440640</PagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2462	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2466	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2472	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 34 00 38 00 38 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3448832</PeakPagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2564	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2568	2	09 00		success or wait	3	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2574	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 33 00 34 00 34 00 30 00 36 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3440640</PrivateUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2646	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2650	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2654	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2700	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2704	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2708	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2738	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2742	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2748	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2788	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2792	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2800	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2830	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2834	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2842	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2912	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2916	2	09 00		success or wait	4	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	2924	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3014	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3018	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3026	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 30 00 34 00 39 00 33 00 38 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6049380</Uptime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3086	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3176	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3240	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	6DF4497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3298	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3388	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3392	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3402	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3476	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3480	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3490	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 39 00 37 00 30 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>49709</PageFaultCount>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3566	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3570	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3580	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 32 00 33 00 37 00 39 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>102379520</PeakWorkingSetSize>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3680	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3684	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3694	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 32 00 30 00 31 00 34 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>102014976</WorkingSetSize>	success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3778	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3782	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3792	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 36 00 37 00 37 00 32 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 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>96772 8</QuotaPeakPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3906	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3910	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	3920	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 31 00 38 00 33 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 >921832</Q uotaPagedPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4018	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4022	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4032	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedP oolUsage>70 736</QuotaPeakNonPag edPoolUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4156	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4160	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4170	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 38 00 35 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUs age>68560< /QuotaNonPagedPoolUsa ge>	success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4278	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4282	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4292	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 35 00 30 00 37 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>342507 52</PagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4370	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4374	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4384	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 34 00 31 00 38 00 31 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35 418112</P eakPagefileUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4478	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4482	2	09 00		success or wait	5	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4492	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 35 00 30 00 37 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3425075 2</PrivateUsage>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4566	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4570	2	09 00		success or wait	4	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4578	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation >	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4624	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4628	2	09 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4634	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4676	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4680	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4684	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4716	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4720	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4722	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4764	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4768	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4770	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4808	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4812	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4816	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4868	4	0d 00 0a 00		success or wait	9	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4872	2	09 00		success or wait	18	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	4876	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 71 00 6a 00 72 00 4f 00 57 00 43 00 43 00 45 00 35 00 38 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>qjrOWCCE58.exe</Parameter0>	success or wait	9	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	5594	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	5598	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	5600	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	5640	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	5644	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	5646	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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	5684	4	0d 00 0a 00		success or wait	6	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	5688	2	09 00		success or wait	12	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	5692	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6246	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6250	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6252	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6292	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6296	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6298	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6336	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6340	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6344	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6438	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6442	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6446	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 68 00 6e 00 74 00 71 00 73 00 70 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>hntqsp, Inc.</SystemManufacturer>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6552	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6556	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6560	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 68 00 6e 00 74 00 71 00 73 00 70 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>hntqsp7,1</SystemProductName>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6656	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6660	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6664	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6784	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6788	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6792	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 30 00 34 00 37 00 35 00 37 00 30 00 31 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1604757010</OSInstallDate>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6874	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6878	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6882	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6984	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6988	2	09 00		success or wait	2	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	6992	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7060	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7064	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7066	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7106	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7110	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7112	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7146	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7150	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7154	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</UEFI SecureBootEnabled>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7250	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7254	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7256	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7292	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7296	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7298	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7322	4	0d 00 0a 00		success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7326	2	09 00		success or wait	6	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7330	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 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000B</Flags>	success or wait	3	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7588	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7592	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7594	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7620	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7624	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7626	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 30 00 35 00 54 00 31 00 32 00 3a 00 34 00 30 00 3a 00 33 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-05T12:40:38Z">	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7726	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7730	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7734	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 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 35 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 32 00 31 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 32 00 31 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="395" PID="1592" UptimeMS="2218" TimeSinceCreationMS="2218" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	7996	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8000	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8004	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	6DF4497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8024	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8028	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8030	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8068	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8072	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8074	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8112	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8116	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8120	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 64 00 32 00 61 00 65 00 39 00 35 00 37 00 2d 00 34 00 63 00 35 00 61 00 2d 00 34 00 62 00 66 00 30 00 2d 00 38 00 33 00 63 00 63 00 2d 00 34 00 30 00 63 00 33 00 32 00 34 00 31 00 39 00 37 00 32 00 64 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>cd2ae957-4c5a-4bf0-83cc-40c3241972d9</Guid>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8218	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8222	2	09 00		success or wait	2	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8226	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 30 00 35 00 54 00 31 00 32 00 3a 00 34 00 30 00 3a 00 33 00 38 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>2022-05-05T12:40:38Z</CreationTime>	success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8324	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8328	2	09 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8330	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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8370	4	0d 00 0a 00		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5015.tmp.WERInternalMetadata.xml	8374	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	6DF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER51AC.tmp.xml	0	4704	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_19545302\Report.wer	0	2	fd fd		success or wait	1	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_19545302\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	165	6DF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_qjrOWCCE58.exe_455362eeffb32f0bf40f06cd73c56872c5d9440_dba93c7d_19545302\Report.wer	10890	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 36 00 31 00 34 00 38 00 39 00 39 00 35 00 35 00 35 00	MetadataHash=-614899555	success or wait	1	6DF4497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a2ddc94a-378c-4111-0081-e5ccc0ecd0c1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF636BF	unknown
\REGISTRY\A\{a2ddc94a-378c-4111-0081-e5ccc0ecd0c1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF636BF	unknown
\REGISTRY\A\{a2ddc94a-378c-4111-0081-e5ccc0ecd0c1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF443D1	unknown

Analysis Process: cmd.exe PID: **6492**, Parent PID: **1592**

General

Target ID:	26
Start time:	05:40:40
Start date:	05/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c taskkill /im "qjrOWCCE58.exe" /f & erase "C:\Users\user\Desktop\qjrOWCCE58.exe" & exit
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: conhost.exe PID: **6568**, Parent PID: **6492**

General

Target ID:	27
Start time:	05:40:42
Start date:	05/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: taskkill.exe PID: **6612**, Parent PID: **6492**

General

Target ID:	29
Start time:	05:40:43
Start date:	05/05/2022
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im "qjrOWCCE58.exe" /f
Imagebase:	0xc0000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
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

Disassembly

No disassembly