ID: 635066
Sample Name:
OR09876545890000987654O.exe
Cookbook: default.jbs
Time: 12:12:20
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

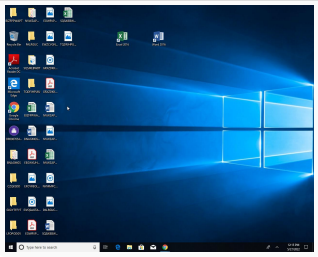
Windows Analysis Report

OR09876545890000098765 40.exe

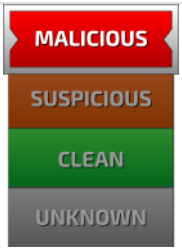
Overview

General Information

Sample Name:	OR09876545890000098765 40.exe
Analysis ID:	635066
MD5:	cb490dd90ce8d9..
SHA1:	1557b8f1f9c2879..
SHA256:	c0f90aecb695c9...
Tags:	AgentTesla exe
Infos:	



Detection



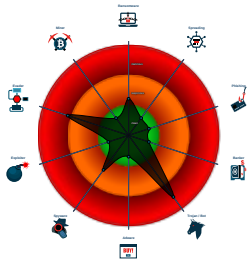
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Yara detected AgentTesla
- Multi AV Scanner detection for drop...
- Machine Learning detection for sam...
- Found evasive API chain (may stop...
- Yara detected Generic Downloader
- Machine Learning detection for drop...
- Uses 32bit PE files
- Yara signature match
- One or more processes crash

Classification



Process Tree

- **System is w10x64**
- OR09876545890000098765 40.exe (PID: 6300 cmdline: "C:\Users\user\Desktop\OR09876545890000098765 40.exe" MD5: CB490DD90CE8D9D11AADB9765ABBE5E5)
  - dktozm.exe (PID: 6336 cmdline: C:\Users\user\AppData\Local\Temp\dktozm.exe C:\Users\user\AppData\Local\Temp\tweziehjnh MD5: 685EB78DF42DD988151ECF00D69BBBF8)
    - dktozm.exe (PID: 6372 cmdline: C:\Users\user\AppData\Local\Temp\dktozm.exe C:\Users\user\AppData\Local\Temp\tweziehjnh MD5: 685EB78DF42DD988151ECF00D69BBBF8)
  - vxmtbmahtsqaf.exe (PID: 6584 cmdline: "C:\Users\user\AppData\Roaming\wyimvgfphnjxg\vxmtbmahtsqaf.exe" MD5: 685EB78DF42DD988151ECF00D69BBBF8)
    - WerFault.exe (PID: 6056 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6584 -s 636 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - vxmtbmahtsqaf.exe (PID: 6776 cmdline: "C:\Users\user\AppData\Roaming\wyimvgfphnjxg\vxmtbmahtsqaf.exe" MD5: 685EB78DF42DD988151ECF00D69BBBF8)
    - WerFault.exe (PID: 3976 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6776 -s 176 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "muhasebe@parkhotelizmir.com",
  "Password": "zHhYkTCp0(bk",
  "Host": "mail.parkhotelizmir.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.255113669.0000000000A20000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.255113669.0000000000A20000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.255113669.0000000000A20000.00000004.00001000.00020000.00000000.sdmp	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x423c7:$s1: get_kbok • 0x42d1c:$s2: get_CHoo • 0x43977:$s3: set_passwordIsSet • 0x421cb:$s4: get_enableLog • 0x46893:$s8: torbrowser • 0x4526f:$s10: logins • 0x44be7:$s11: credential • 0x415b7:$g1: get_Clipboard • 0x415c5:$g2: get_Keyboard • 0x415d2:$g3: get_Password • 0x42bca:$g4: get_CtrlKeyDown • 0x42bda:$g5: get_ShiftKeyDown • 0x42beb:$g6: get_AltKeyDown
Process Memory Space: dktozm.exe PID: 6336	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.dktozm.exe.a31658.0.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.dktozm.exe.a31658.0.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.dktozm.exe.a31658.0.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
1.2.dktozm.exe.a31658.0.raw.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30d6f:$s1: get_kbok • 0x316c4:$s2: get_CHoo • 0x3231f:$s3: set_passwordIsSet • 0x30b73:$s4: get_enableLog • 0x3523b:$s8: torbrowser • 0x33c17:$s10: logins • 0x3358f:$s11: credential • 0x2ff5f:$g1: get_Clipboard • 0x2ff6d:$g2: get_Keyboard • 0x2ff7a:$g3: get_Password • 0x31572:$g4: get_CtrlKeyDown • 0x31582:$g5: get_ShiftKeyDown • 0x31593:$g6: get_AltKeyDown
1.2.dktozm.exe.a31658.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 8 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Stealing of Sensitive Information

Yara detected AgentTesla

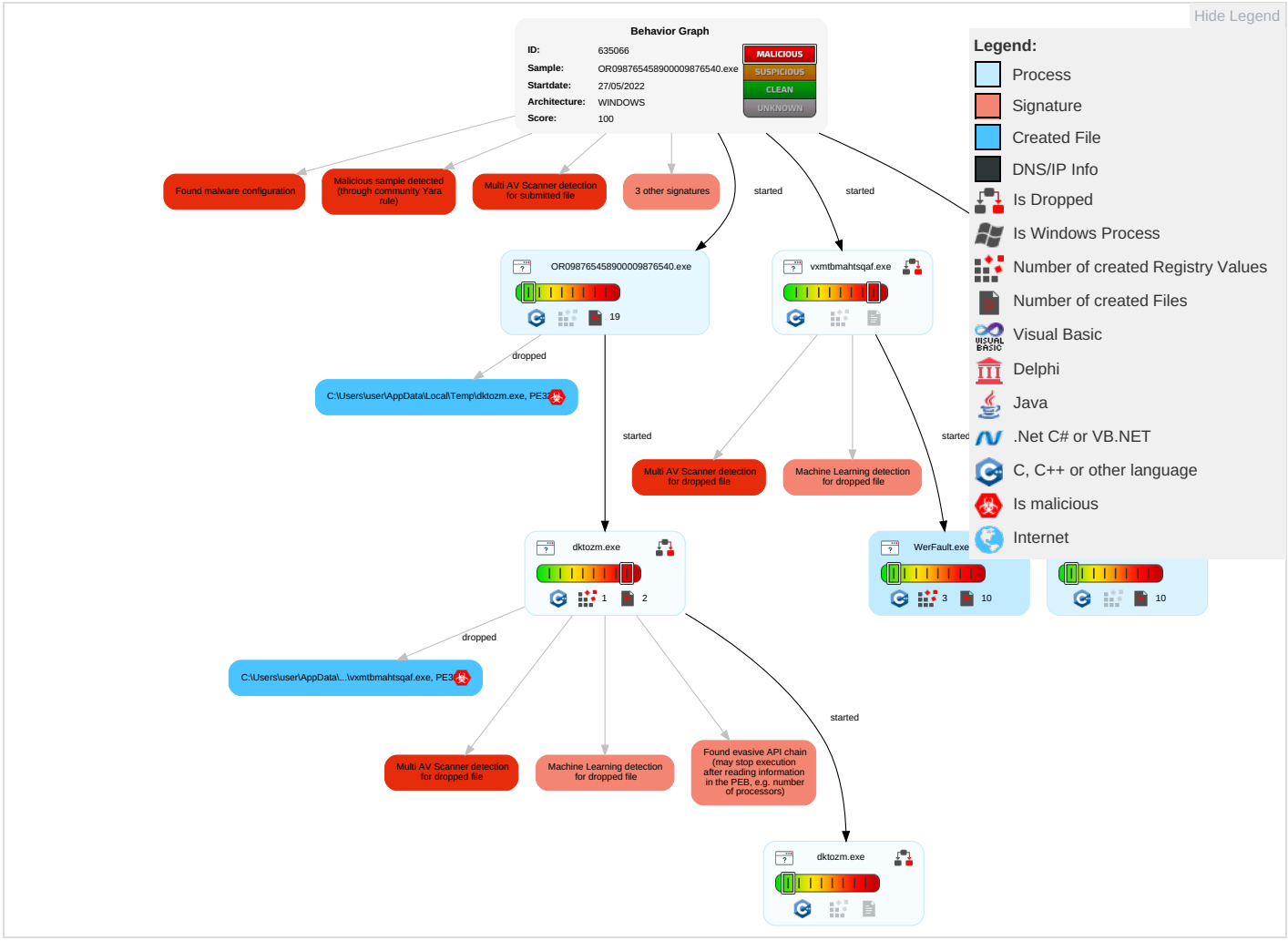
Remote Access Functionality

Yara detected AgentTesla

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	2 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 1 Process Injection	1 Masquerading	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 2 Native API	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 1 Process Injection	LSASS Memory	1 3 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	1 Clipboard Data	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)	Binary Padding	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

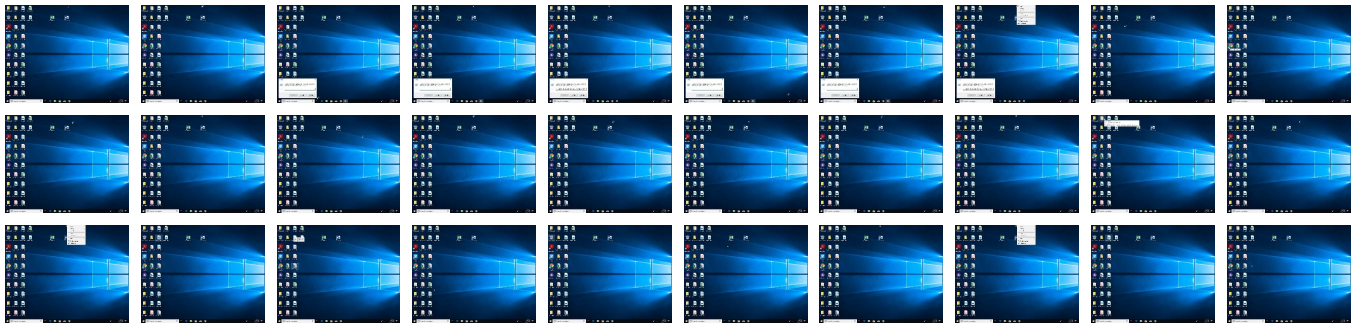
Behavior Graph



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
OR0987654589000098765 40.exe	29%	Virustotal		Browse
OR0987654589000098765 40.exe	27%	ReversingLabs	Win32.Trojan.AgentTesla	
OR0987654589000098765 40.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\dktozm.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\wyimvgfphnjxg\vxmtbmahtsqaf.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\dktozm.exe	40%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\dktozm.exe	27%	ReversingLabs	Win32.Trojan.Jaik	
C:\Users\user\AppData\Roaming\wyimvgfphnjxg\vxmtbmahtsqaf.exe	40%	Virustotal		Browse
C:\Users\user\AppData\Roaming\wyimvgfphnjxg\vxmtbmahtsqaf.exe	27%	ReversingLabs	Win32.Trojan.Jaik	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	dktozm.exe, 00000001.00000002.255113669.0000000000A20000.00000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635066
Start date and time: 27/05/202212:12:20	2022-05-27 12:12:20 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OR098765458900009876540.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:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/13@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 96.3% (good quality ratio 90.1%) • Quality average: 78.1% • Quality standard deviation: 29%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.42.73.29, 20.189.173.22, 52.152.110.14, 20.54.89.106, 40.125.122.176, 20.223.24.244, 52.242.101.226
- Excluded domains from analysis (whitelisted): fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, onedsblobprdwus17.westus.cloudapp.azure.com, arc.msn.com, ris.api.iris.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
12:13:25	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run xnfumqdlkjxkua C:\Users\user\AppData\Roaming\wyimvgfphnjxg\vxmtbmahtsqaf.exe
12:13:34	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run xnfumqdlkjxkua C:\Users\user\AppData\Roaming\wyimvgfphnjxg\vxmtbmahtsqaf.exe
12:14:00	API Interceptor	2x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vxmtbmahtsqaf.ex_cb9e76617add17783445895d2c3df37ac7ad2b_79937427_0fb4cdeb\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):	0.9311478251749132
Encrypted:	false
SSDEEP:	192:jsPMipweHv8ejcljb7aRq/u7sPS274Itd:APMipwWv8ejclj/P/u7sPX4Itd
MD5:	85F1C3E2A2BD3CC87CD6EE3DE8ACD1FC

SHA1:	31E9876651340526DF41D043D41B77E8387AD597
SHA-256:	E5618E7F21BE742EE2B66A2B5D8678B4993B2E82DCEFF0BDAA9E3EE3786BD1EF
SHA-512:	514729E7DD77686F0FE62791375E89B4B7FF8CC37DF479177581D1D9CC85D3BB7051DEFBA9DE44DE47FE0CAA4E98577990AE82C554CFC0003109F4DD566E25 6
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.8.1.5.2.4.4.2.3.3.9.8.6.3.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.8.1.5.2.4.4.4.3.5.5.4.4.8.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.3.b.c.5.d.7.a.-.e.f.e.a.-.4.d.6.b.-.9.5.4.c.-.1.3.2.6.2.a.c.3.d.5.3.2.....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.=.b.5.6.3.b.4.0.b.-.9.6.c.9.-.4.0.7.6.-.b.b.3.f.-.0.f.4.9.2.a.2.d.7.f.f.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.=.v.x.m.t.b.m.a.h.t.s.q.a.f...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.7.8.-.0.0.0.1.-.0.0.1.d.-.a.0.f.d.-.2.5.e.1.f.d.7.1.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.b.8.1.d.f.f.f.7.8.8.7.6.5.7.2.f.4.4.c.0.2.f.9.2.6.2.e.1.d.3.8.0.0.0.0.f.f.f.f.!.0.0.0.0.d.8.2.8.2.c.8.e.5.a.7.0.d.8.d.5.f.9.d.a.1.4.9.e.a.f.9.4.0.f.d.c.3.6.6.a.8.7.5.6.!.v.x.m.t.b.m.a.h.t.s.q.a.f...e.x.e.....T.a.r.g.e.t.A.p.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vxmtbmahtsqaf.ex_cb9e76617add17783445895d2c3df37ac7ad2b_799374

27_1794bb3d\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):	0.9380095501138146
Encrypted:	false
SSDEEP:	192:h7HG4MiPweHv8ejcljRkKDq/u7sPS274ltd:tHG4MiPwWv8ejcljTu/u7sPX4ltd
MD5:	B45E212FDB7EE4DB50E049AC0814264E
SHA1:	27E3D033E3DE5F302FF9004A17AFA8B5B8B4CCFF
SHA-256:	E1C6BBCB32E31C7EF7F08BFE1768E6C9CA785284A107842F3A2044C9BC547F42
SHA-512:	0C3EEC0B760572237F3EC21C9D0F26CE962DC69F45BD69725C31CD0E6B1A6BD80671BB9B61AB1B9836DD62DA7E5ECDECE35E7BF092809E11B482A3924D2D9 1A0
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.8.1.5.2.4.3.3.8.3.4.9.3.0.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.8.1.5.2.4.3.9.3.8.1.8.1.4.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.6.5.e.b.1.a.b.-.8.b.4.d.-.4.a.e.1.-.9.5.b.3.-.c.4.0.7.3.7.4.7.1.7.b.b.....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.=.e.8.d.2.b.0.2.1.-.3.d.c.e.-.4.f.a.6.-.b.e.7.3.-.8.4.c.f.1.4.8.7.2.2.a.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.v.x.m.t.b.m.a.h.t.s.q.a.f...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.b.8.-.0.0.0.1.-.0.0.1.d.-.b.b.a.e.-.4.1.d.c.f.d.7.1.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.b.8.1.d.f.f.f.7.8.8.7.6.5.7.2.f.4.4.c.0.2.f.9.2.6.2.e.1.d.3.8.0.0.0.0.f.f.f.f.!.0.0.0.0.d.8.2.8.2.c.8.e.5.a.7.0.d.8.d.5.f.9.d.a.1.4.9.e.a.f.9.4.0.f.d.c.3.6.6.a.8.7.5.6.!.v.x.m.t.b.m.a.h.t.s.q.a.f...e.x.e.....T.a.r.g.e.t.A.p.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri May 27 19:13:54 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	47428
Entropy (8bit):	1.7821677765394452
Encrypted:	false
SSDEEP:	192:GxRgEbGlEyYjcQOcR1xTEVOBW2yIN5Zlo9AsDPp2eTGL:WKEyyzwczxTEVOB7yo5Zloi43Ts
MD5:	F7A766929987999794 70CEC931C45034
SHA1:	B4F10A6BE024B3A2BEF30FE742DA3FAC51BE4D5B
SHA-256:	B25FE543B8D2DAF512C479772D276DE13AA195F7897145E6E1CFCB2D5381DC14
SHA-512:	C41A373713695FD97393F8A5F8DFA78F4F9866B5E35326BA73EC23E9975A72EDDF463C2F23734C058F6FF754E782D896120DCDB7BB62AB59BF85485616472BA0
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....".b.....R0.....T.....8.....T.....8.....U.....B.....P.....GenuineIntelW.....T.....".b..... .....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\WERA536.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):	3.69419278114427
Encrypted:	false

SSDEEP:	192:Rrl7r3GLNieK6G56YWMSUyjrgmf3SccCpDgV89bqrsfo4um:RrlsNir6o6YNSUyPgmf3Sc7qwfoI
MD5:	E599241B68B02B574619755E424D0369
SHA1:	9EC429B845615F1441E0246ED9CAA3FAC6A1843E
SHA-256:	D71AB80C38DAF462C396486BB45260993F54DDFDA48F3EA78E6147B84A846E29
SHA-512:	AF88CACD4BAAC18AE84CED2CF9B016BCEB4B0D0111FFDDE2C1A34DB300B4F26EACA613187AC885CE9598F16432A7A9FE5A2A9E7BA0F116E34C9621791F5EB8CF
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.5.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA19.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4685
Entropy (8bit):	4.430789063702757
Encrypted:	false
SSDEEP:	48:cvIwSD8zsoJgtWI9DLWgc8sqYjX8fm8M4Jv1FX+q8veEbFeGLKCvkd:uITfug6grsqYoJ/KnbFRL7vkd
MD5:	1816EDBA538B2E76FF10329EC3D6F6A9
SHA1:	215C8AF61A69A3831D84C31A787511EAD030A41C
SHA-256:	980E1913C733AFF961E8F9E9F83A506C60DE3688744FF4D33FE88C628DD7EBAE
SHA-512:	48EEAEFB5D3CB8A93829BE315F05DA8363CDD86E4DBE3BB27457F25D10C5EC45059D9E2E9C90ECC898383AE963BA8DF0105E9E88F7A9E27F2608F7C053C513CD
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1533864" />.. <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\WERC0CB.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri May 27 19:14:03 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	38540
Entropy (8bit):	1.9579536066282275
Encrypted:	false
SSDEEP:	192:jkRZ6QB9dPeOIRiVA96qAdH7dv/7X8yLR4:oPLxPZIAVA96qAdH7dv/4
MD5:	933DFE279B92B4B539715271C1428B80
SHA1:	44B168FF2A0922AE28E5666CBAD0EAA2B44D63CC
SHA-256:	1E7B9E8242796B2B9617B106A3E7D894B70998503B8F4B2955B2B56C6B62DBF2
SHA-512:	8A6A6CB417AD858B1379705A5360733362099CED67E0C0B0601569198F0F53A7E9ADFE216C9E7C3BB88066C0EB917ABAA6B2DF0A4AE0D48F923B77D2365B901A
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....".b.....,.....T.....8.....T..... ...l~.....0.....U.....B.....GenuineIntelW.....T.....x....".b..... .....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\WERC5BE.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):	8410
Entropy (8bit):	3.6935135824172765

Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipb6iV6YW/SUFQOgmf3SccCpDgcq89b+osf9Rqm:RrlsNil6iV6YuSUFQOgmf3SclT+bf99
MD5:	E9118A1901C356681D0B1467AE555510
SHA1:	86B3682858CFF23C0072A79844BF3C6AF807AFB4
SHA-256:	4057C7935F0F6E4DFFC68306BFF5970E67FD2437D328C1FA405F6B91AA3B0042
SHA-512:	43F03F0DF1690959A8533FD21B5FD0F081A9C9407C03D8B0CCB7CEE0BE61C36CFAD714A662463F52EEAF9B8FB9A80A4D4584B4941A73C89A1B168B700923624 3
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.7.7. 6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC745.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4685
Entropy (8bit):	4.4327683606503605
Encrypted:	false
SSDEEP:	48:cvIwSD8zsoJgtWI9DLWgc8sqYjD8fm8M4Jv1FF+q8veJFeGLKCvgd:uITfug6grsqYsJ9K8FRL7vgd
MD5:	242123207DC4CB278704A0D068BD21E7
SHA1:	02087A9B0B4873D1039EC444062E2EFB216B9389
SHA-256:	4FE98854E7F0C473441C924E8AC95BCCF9FCEC1A593319D5F821B2838D16320E
SHA-512:	0E8E457BCB117C646153040249630BD01ACCEB7E8CCB01EA3BFA32D482DBA14A78C9830C0E78BD25A379A00595CCF0B38039D4EC7359A1474146269C2B9241 4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" /> .. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1533864" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0- 11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Temp\dktozm.exe

Process:	C:\Users\user\Desktop\OR0987654589000098765 40.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	135168
Entropy (8bit):	6.407323687210526
Encrypted:	false
SSDEEP:	1536:/VTOG+x8+YaGDARvmJVBqNvnlajcCOO0LdXU8JiA1OySuJuRqSnakMP1BOBYCH4E:wfbnR6BqNvncvhw4u+qSng1kGCUHt
MD5:	685EB78DF42DD988151ECF00D69BBBF8
SHA1:	D8282C8E5A70D8D5F9DA149EAF940FDC366A8756
SHA-256:	17B6C8284FCA1E77875DA1945DE13B20EF80E9422E2284EF6DC9FF1264A70D77
SHA-512:	C4EBB121602A484144DBDF4F23FB9093513BE870C04AAA082CDBF8C22583CDBF383669E483182CBCB7E6F94E225E68643553DABB3CDB9E3E6B80BE0D2284BD 3D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 27%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G..8.~ck.~ck.~ck.,.k.~ck.,.k.~ck.,.kp~ck..bj.~ck.~bk.~ck..gj.~ ck...k.~ck..aj.~ckRich.~ck.....PE..L....<.b.....w.....@.....p.....@.....|.....P.....`.....x...T..... .....0...@.....4.....text..... ..`.rdata...P.....R.....@..@.data....1.....@....rsrc.....P.....@..@.reloc.... ...`.....@..B..... .....

C:\Users\user\AppData\Local\Temp\hgwowmqnjcs91i7x

Process:	C:\Users\user\Desktop\OR0987654589000098765 40.exe
File Type:	data

Category:	dropped
Size (bytes):	293375
Entropy (8bit):	7.957092929980963
Encrypted:	false
SSDEEP:	6144:24KAZdkDQ6KmS+bPFFfuDDkLL90wa0rjHcXRvkm3RwxOZ7AeAKXyBJ92po:yAZCQfmS+bt5u8SHsLoRsmBlisSQJ95
MD5:	DA1FBC1E880C5844C5DE93D355DC623F
SHA1:	35902D81B16D200E9CAE241B133CE5C199566DC7
SHA-256:	8181B3C286A944B8949E3633E97D464F17F9C986160955065D65025A249F7C54
SHA-512:	0BD817CD578E8384C7829CBE62E0FDB59C77F048226D7927899C8886C05F242DC143A846EE90DCEFDEFB12E8E9FF1FC0461BFC2F01741C4CB80CB8FACCF085D
Malicious:	false
Reputation:	low
Preview:	.;(.M\]....:3..;9..6D.....A."}.H...}...v.....-fO.(..oF...s[\ a..3I..+y;....-*6L..A.=..Z..Y-..Co...Z..4.|..-..Gm.B....@..3.z..7.E.E..o.2.?3.).%..e.-j....+.$..b.~.+.Dv....`.|.S...%r.n...].hq.L.....a.....T.&*8Al9..A.....X}.....3.....6+j=.1.Y..=.].yS.Y}3.";9.j6..J.T.TA."..H.....-.O.0..o..wd.4 ...yq....Y.r2..?.3.Zr/....!"I..O....Ih.T.....N...B.....>=.D..4...s.!H.Bp...6U3... .....CPaG].\.{t6.S.1...:GY`....`o.#.K...I.....s.....{..V.D..A P.....N.5B...-.&.c....j=...Y.Ol\].1..Y.3.";9..6D.....A....A....G.....fO.(..o...d84.....C.F.Y.eH...W3..r/.,...!.I..O..n.B....xx...N.q'#..8.....`4...s>...Bp...6U.... .....CPaG].C...t6.S.1...:GY`....`o.#.K...IL.r...s.....D..A P.....N.5B...-.&....6+j=..)Y.OM\]....Y}3.";9..6D.....A."}.H...}...v.....-fO.(..o...d84 ....q....Y.rP....3.Zr/.....!.I..O..n.I..T....4.N...B.....4...s>...Bp...6U3... .....CPaG].C...t6.S.1...:GY`....`o.#.K...IL.r...s.....D..A P..

C:\Users\user\AppData\Local\Temp\nsa28F1.tmp

Process:	C:\Users\user\Desktop\OR098765458900009876540.exe
File Type:	data
Category:	dropped
Size (bytes):	440782
Entropy (8bit):	7.672595381068025
Encrypted:	false
SSDEEP:	12288:FAZCQfmS+bt5u8SHsLoRsmBlisSQJ9PycWVJ:FAZVfmS+btM8pLo1Blis/
MD5:	35B2CAB2BB1FC169A7D95B88797261D5
SHA1:	C5B56CF62B59B5E57692791B94C01BB910A5A588
SHA-256:	3227DA1033099DB1F8DF206C3CA639EDA1770DE2E4AFBAC8477854BBB70576F3
SHA-512:	E23AA89C59EC2F44BB2AE5C506EBC84E59216646C171EF333F1F41BF27A7F559F52C44A95FB6FB2BCFA8E574261104A759C9DD3A2552ABBBE804904EB982AB9B
Malicious:	false
Preview:	7.....,.....8.....q.....7..... .....B.....}...j.....].... ....

C:\Users\user\AppData\Local\Temp\tweziehjnh

Process:	C:\Users\user\Desktop\OR098765458900009876540.exe
File Type:	data
Category:	dropped
Size (bytes):	7816
Entropy (8bit):	6.058140230956638
Encrypted:	false
SSDEEP:	192:/B2CPdrYpMPFgH5UrdKb8kMCw/T43Ed6c+ghNPPtNNeAe5j1YZ:tY6PFgZUrdJ7FeAe5j1G
MD5:	D6431A217236A88180593D1116640D96
SHA1:	9332040CF2A4C7CA21A146C4F999AB3977C45BEC
SHA-256:	0828DFF4118755DE9226F4A9EF994BA7D27E19DAF83D9B5973896E3F754350AF
SHA-512:	91852E6CAE7546C9CDABF2AE87D2E4BE5B44A7BB79ABA8A3BC331B0FE35B82603D7C552DE6A587F60A7440F336214254CABB4646DCF4BAD7458D2B9BC7EF62C0
Malicious:	false
Preview:	a.....d.d.....H..h..H..`..O.....`.....p..t.....`n.....x..|.....`y.....@..D.....`T.....H..L.....H...1..h..l...`..A..`..d..`....l.z....`.....J.....l...`.....C...p..x..@...H...h...`..... .f.....p.....`....O.....C.....AJ....d....H.....l..l.....AJ...N.`....`....J....w.`..`....J....3.`...`...J....d.d...H..`O.....p.....N.....cl`.....H....1...A...p...t..`1..li... p...t....H...p...w.`C....`z.....c...`....`.....c.O.....AJ....d.d..H..`O.....H.....N.....cl`1....H.....1...A...H...L..1..li...H...L..1..yi..H...L...A...z...H..L..`1..li...H...L....H... H..N.`j....`a.....`....c.....`.....c.O.....AJ....d.d.O.....l.....N.....cl`*....H....1...A...l...`..1..li...l...`....H...l....3.`.....`.....c.....`_..

C:\Users\user\AppData\Roaming\wyimvgfphnjxg\vxmtbmahtsqaf.exe

Process:	C:\Users\user\AppData\Local\Temp\dktozm.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	135168
Entropy (8bit):	6.407323687210526
Encrypted:	false

SSDEEP:	1536:/VTOG+x8+YaGDARvmJVBqNvnlajcCOO0LdXU8JiA1OySuJuRqSnakMP1BOBYCH4E:wfbnR6BqNvncvhw4u+qSng1kGCUHt
MD5:	685EB78DF42DD988151ECF00D69BBBF8
SHA1:	D8282C8E5A70D8D5F9DA149EAF940FDC366A8756
SHA-256:	17B6C8284FCA1E77875DA1945DE13B20EF80E9422E2284EF6DC9FF1264A70D77
SHA-512:	C4EBB121602A484144DBDF4F23FB9093513BE870C04AAA082CDBF8C22583CDBF383669E483182CBCB7E6F94E225E68643553DABB3CDB9E3E6B80BE0D2284BD3D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 27%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G..8.~ck.~ck.~ck.,.k.~ck.,.k.~ck.,.kp~ck..bj.~ck.~bk.~ck..gj.~ck...k.~ck..aj.~ckRich.~ck.....PE..L....<.b.....w.....@.....p.....@.....|.....P.....`.....x...T.....0...@.....4.....text..... ..`.rdata...P.....R.....@..@.data....1.....@....rsrc.....P.....@..@.reloc....`.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.159985869716827
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	OR098765458900009876540.exe
File size:	511491
MD5:	cb490dd90ce8d9d11aadb9765abbe5e5
SHA1:	1557b8f1f9c2879a8de75689530f78d796d8fc04
SHA256:	c0f90aecb695c93c21e13bbb346f794928bd4dfdde1c3c88c70f62acaf1d368e
SHA512:	13b45813a974c849e458190a62ff1d23f32ec4e05d6786b81196082a5983ac7c63ab2b8e62953b3299067fa7a33d65cd6503762e927e1a35752bf516817f4d34
SSDEEP:	6144:s0YynsIMquMA3WcHWlZMZ6hBTQaN2SX1RtUfVYuoPgymDvTvPlzwalv6:5wqlWMCZMZW2aNl1RtsVYuRymDbI8l6
TLSH:	69B457E42343C2B5EC05A73918D28921F2366F862D20D97E2602BBFAFF7F19B54151E5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qJ...$...$...$./.{...$...%.;.$.".y...$..3....$.f."...$.Rich..$.....PE..L.....iF.....Z.....

File Icon

Icon Hash:	70ccb2b0e8e8e431

Static PE Info

General

Entrypoint:	0x4032fa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4669CEB6 [Fri Jun 8 21:48:38 2007 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0

Import Hash:	55f3dfd13c0557d3e32bcbc604441dd3

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409170h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push ebx
call dword ptr [00407278h]
mov dword ptr [00423FD4h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F4E8h
call dword ptr [00407154h]
push 0040922Ch
push 00423720h
call 00007F4CD8B4F2E8h
call dword ptr [004070B4h]
mov edi, 00429000h
push eax
push edi
call 00007F4CD8B4F2D6h
push ebx
call dword ptr [00407108h]
cmp byte ptr [00429000h], 00000022h
mov dword ptr [00423F20h], eax
mov eax, edi
jne 00007F4CD8B4CB4Ch
mov byte ptr [esp+14h], 00000022h
mov eax, 00429001h
push dword ptr [esp+14h]
push eax
call 00007F4CD8B4EDC9h
push eax
call dword ptr [00407218h]
mov dword ptr [esp+1Ch], eax
jmp 00007F4CD8B4CBA5h
cmp cl, 00000020h
jne 00007F4CD8B4CB48h
inc eax
cmp byte ptr [eax], 00000020h
je 00007F4CD8B4CB3Ch
cmp byte ptr [eax], 00000022h
mov byte ptr [esp+14h], 00000020h
jne 00007F4CD8B4CB48h
inc eax
mov byte ptr [esp+14h], 00000022h
cmp byte ptr [eax], 0000002Fh
jne 00007F4CD8B4CB75h

Instruction
inc eax
cmp byte ptr [eax], 00000053h
jne 00007F4CD8B4CB50h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x73a0	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x2bcf8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x288	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x59ac	0x5a00	False	0.668142361111	data	6.45807821776	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x117a	0x1200	False	0.4453125	data	5.17513527374	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1afd8	0x400	False	0.6015625	data	4.98110806401	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x2bcf8	0x2be00	False	0.200710024929	data	4.39704209832	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2c310	0x3d2e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x30040	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x40868	0x94a8	data	English	United States
RT_ICON	0x49d10	0x5488	data	English	United States
RT_ICON	0x4f198	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 16777215, next used block 4294967040	English	United States
RT_ICON	0x533c0	0x25a8	data	English	United States
RT_ICON	0x55968	0x10a8	data	English	United States
RT_ICON	0x56a10	0x988	data	English	United States
RT_ICON	0x57398	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x57800	0x100	data	English	United States
RT_DIALOG	0x57900	0x11c	data	English	United States
RT_DIALOG	0x57a20	0x60	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0x57a80	0x84	data	English	United States
RT_MANIFEST	0x57b08	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, CreateFileA, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, CloseHandle, ExitProcess, GetWindowsDirectoryA, GetTempPathA, GetCommandLineA, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, SetErrorMode, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, CopyFileA
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, CreateDialogParamA, DestroyWindow, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

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

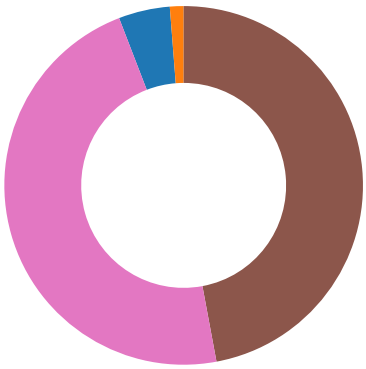
Network Behavior

No network behavior found

Statistics

Behavior

- OR098765458900009876540.exe
- dktozm.exe
- dktozm.exe
- vxmtbmahtsqaf.exe
- vxmtbmahtsqaf.exe
- WerFault.exe
- WerFault.exe



Click to jump to process

System Behavior

Analysis Process: OR098765458900009876540.exe PID: 6300, Parent PID: 4376

General

Target ID:	0
Start time:	12:13:22
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\OR098765458900009876540.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\OR098765458900009876540.exe"
Imagebase:	0x400000
File size:	511491 bytes
MD5 hash:	CB490DD90CE8D9D11AADB9765ABBE5E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4032ED	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsa28F0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40582D	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsa28F1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40582D	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsv2921.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40582D	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsv2921.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\hgwowmqnjcs91i7x	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4057F7	CreateFileA
C:\Users\user\AppData\Local\Temp\tweziehjnh	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4057F7	CreateFileA
C:\Users\user\AppData\Local\Temp\dktozm.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4057F7	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsa28F0.tmp	success or wait	1	40345C	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsv2921.tmp	success or wait	1	40544C	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsa28F1.tmp	0	20131	37 11 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 01 00 00 00 fd 05 00 00 38 00 00 00 fd 0b 00 00 00 00 00 00 71 10 00 00 01 00 00 00 37 11 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	7,8q7	success or wait	20	4031E9	WriteFile
C:\Users\user\AppData\Local\Temp\hgwowmqnjcs91i7x	0	16384	fd 3b 28 a5 4d 5c 5d 96 fd fd fd 3a 33 fd fd 3b 39 2e fd 36 44 fd fd fd 14 1a 04 fd 41 04 22 7d fd 48 4e fd 0a 7d d6 fd fd 76 fd 10 fd fd fd fd 1e 2d 66 4f fd 28 fd fd 6f 46 fd 06 2e 73 5b 5c 20 61 19 fd 33 49 fd 08 2b 79 3b 13 fd fd 18 2d 2a 36 4c fd fd 41 fd 3d fd fd 5a fd fd 59 2d fd fd 43 6f fd fd fd 5a fd fd 34 fd 7c fd fd 2d fd 0b 47 6d fd 42 1f fd fd 13 40 7f fd 33 fd 7a fd fd 37 fd 45 fd 45 fd 16 6f fd 32 19 3f 33 18 29 fd 25 fd fd 65 1b 2d 6a 0b fd 0f fd 2b 03 24 db fd 62 fd 7e fd 2b fd 44 76 14 fd fd fd 60 fd 7c fd 53 16 ed fd 25 72 fd 6e fd fd 06 5d fd 68 71 fd 4c fd 13 18 fd fd 61 fd fd fd fd fd 16 1b 54 15 26 2a 38 41 6c 39 11 fd 41 fd fd 95 fd fd 1c 58 7d fd fd fd fd 10 fd 33 69 fd fd fd fd 36 2b 6a 3d	;(M\]:3;9.6DA"}H}v-fO(oF.s[\ a3I+y;-*6LA=ZY-CoZ4|-GmB@3z7EEo2?3)%e-j+$b~+Dv`|S%rn]hqLaT&*8Al9AX}36+j=	success or wait	18	40303D	WriteFile
C:\Users\user\AppData\Local\Temp\tweziehjnh	0	7816	61 fd fd fd fd fd 03 64 0b 64 fd fd fd fd 0b 08 fd fd 48 fb fd 68 fd fd 48 fb fd 60 0b 08 4f 54 fd fd fd fd 0b 08 fd 1d fd fd 1d fd 05 50 fd 60 fd fd fd fd 01 fd 70 01 fd 74 fd 1d fd fd 1d fd 05 50 fd 60 6e fd fd fd 01 fd 78 01 fd 7c fd 1d fd fd 1d fd 05 50 fd 60 79 fd fd fd 01 fd 40 01 fd 44 fd 1d fd fd 1d fd 05 50 fd 60 54 fd fd fd 01 fd 48 01 fd 4c 0b 15 fd fd 1e fd fd fd fd 48 fd fd 44 31 01 fd 68 01 fd 6c 03 78 0b 60 fd fd 41 01 fd 60 01 fd 64 03 fd 60 03 54 05 fd 49 fd 7a fd fd 03 fd 60 fd fd fd 05 fd 4a 01 54 fd fd 01 fd 0b 6c fd fd fd 60 fd fd fd fd 0b fd fd fd 43 fd 17 1d 70 fd 1d 78 fd 1d 40 fd fd 1d 48 fd fd 1d 68 fd fd 1d 60 fd 0d fd 1c fd fd fd 03 fd fd	addHhH`O`pt`nx|`y@D`THLH1hl`A`d`Iz`Jl`Cpx@Hh`	success or wait	1	40303D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\dktozm.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 47 1f 0d 38 03 7e 63 6b 03 7e 63 6b 03 7e 63 6b 0e 2c fd 6b 1b 7e 63 6b 0e 2c fd 6b 0c 7e 63 6b 0e 2c fd 6b 70 7e 63 6b fd 0c 62 6a 10 7e 63 6b 03 7e 62 6b fd 7e 63 6b fd 07 67 6a 02 7e 63 6b fd 07 fd 6b 02 7e 63 6b fd 07 61 6a 02 7e 63 6b 52 69 63 68 03 7e 63 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 3c fd 62 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$G8~ck~ck~ck,k~ck,k~ck,kp~ckbj~ck~bk~ckgj~ckk ~ckaj~ckRich~ckPEL<b	success or wait	9	40303D	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\OR098765458900009876540.exe	unknown	512	success or wait	410	40329A	ReadFile
C:\Users\user\Desktop\OR098765458900009876540.exe	unknown	16384	success or wait	19	40329A	ReadFile
C:\Users\user\AppData\Local\Temp\nsa28F1.tmp	unknown	4	success or wait	1	402FC7	ReadFile
C:\Users\user\AppData\Local\Temp\nsa28F1.tmp	unknown	4407	success or wait	1	40307D	ReadFile
C:\Users\user\AppData\Local\Temp\nsa28F1.tmp	unknown	4	success or wait	3	402FC7	ReadFile
C:\Users\user\AppData\Local\Temp\nsa28F1.tmp	unknown	16384	success or wait	28	403021	ReadFile

Analysis Process: dktozm.exe PID: 6336, Parent PID: 6300

General

Target ID:	1
Start time:	12:13:24
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Temp\dktozm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\dktozm.exe C:\Users\user\AppData\Local\Temp\tweziehjnh
Imagebase:	0x1160000
File size:	135168 bytes
MD5 hash:	685EB78DF42DD988151ECF00D69BBBF8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.255113669.0000000000A20000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.255113669.0000000000A20000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000001.00000002.255113669.0000000000A20000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 40%, Virustotal, Browse • Detection: 27%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wyimvgfphnjxg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A11CA1	CreateDirectoryW
C:\Users\user\AppData\Roaming\wyimvgfphnjxg\vxmtbmahtsqaf.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	A11E55	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wyimvgfphnjxg\vxmtbmahtsqaf.exe	0	135168	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 47 1f 0d 38 03 7e 63 6b 03 7e 63 6b 03 7e 63 6b 0e 2c fd 6b 1b 7e 63 6b 0e 2c fd 6b 0c 7e 63 6b 0e 2c fd 6b 70 7e 63 6b fd 0c 62 6a 10 7e 63 6b 03 7e 62 6b fd 7e 63 6b fd 07 67 6a 02 7e 63 6b fd 07 fd 6b 02 7e 63 6b fd 07 61 6a 02 7e 63 6b 52 69 63 68 03 7e 63 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 3c fd 62 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$G8~ck~ck~ck,k~ck,k~ck,kp~ckbj~ck~bk~ckgj~ckk ~ckaj~ckRich~ckPEL<b	success or wait	1	A11E6A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tweziehjnh	unknown	4096	success or wait	1	116F96C	ReadFile
C:\Users\user\AppData\Local\Temp\tweziehjnh	unknown	4096	success or wait	1	116F96C	ReadFile
C:\Users\user\AppData\Local\Temp\hgwowmqnjcs91i7x	unknown	293375	success or wait	1	A10BD4	ReadFile
C:\Users\user\AppData\Local\Temp\dktozm.exe	unknown	135168	success or wait	1	A11E2B	ReadFile

Registry Activities

Analysis Process: dktozm.exe

PID: **6372**, Parent PID: **6336**

General

Target ID:	2
Start time:	12:13:25
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Temp\dktozm.exe
Wow64 process (32bit):	
Commandline:	C:\Users\user\AppData\Local\Temp\dktozm.exe C:\Users\user\AppData\Local\Temp\tweziehjnh
Imagebase:	
File size:	135168 bytes
MD5 hash:	685EB78DF42DD988151ECF00D69BBBF8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

Analysis Process: vxmtbmahtsqaf.exe PID: **6584**, Parent PID: **3968**

General

Target ID:	5
Start time:	12:13:34
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\wyimvgfphnjxg\vxmtbmahtsqaf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\wyimvgfphnjxg\vxmtbmahtsqaf.exe"
Imagebase:	0xe10000
File size:	135168 bytes
MD5 hash:	685EB78DF42DD988151ECF00D69BBBF8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 40%, Virustotal, Browse • Detection: 27%, ReversingLabs
Reputation:	low

Analysis Process: vxmtbmahtsqaf.exe PID: **6776**, Parent PID: **3968**

General

Target ID:	8
Start time:	12:13:42
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\wyimvgfphnjxg\vxmtbmahtsqaf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\wyimvgfphnjxg\vxmtbmahtsqaf.exe"
Imagebase:	0xe10000
File size:	135168 bytes
MD5 hash:	685EB78DF42DD988151ECF00D69BBBF8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: **6056**, Parent PID: **6584**

General

Target ID:	16
Start time:	12:13:53
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6584 -s 636
Imagebase:	0xa20000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
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	6DBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA19.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA19.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vxmtbmahtsqaf.ex_cb9e76617add17783445895d2c3df37ac7ad2b_79937427_1794bb3d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vxmtbmahtsqaf.ex_cb9e76617add17783445895d2c3df37ac7ad2b_79937427_1794bb3d\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA19.tmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA19.tmp.xml	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER484E.tmp.csv	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER486E.tmp.txt	success or wait	1	6DBD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 fd 22 fd 62 fd 05 12 00 00 00 00 00	MDMP "b	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	7504	6	00 00 00 00 00 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.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 50 1d 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 19 00 00 fd 22 fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 20 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	UBPGenuineIntelWT"b Pacific Standard TimePacific Daylight Time	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	8790	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 fd 1e 00 00 fd 01 00 00 05 00 00 00 01 00 00 00 4c fd fd 00 fd fd fd 00 23 00 00 00 02 02 00 00 34 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++L#4+	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	1620	168	fd 19 00 00 00 00 00 00 09 04 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 00 00 00 00 00 01 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 56 22 00 00	V"	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	12370	20	10 00 00 00 00 fd fd 00 00 00 00 00 fd 04 00 00 56 31 00 00	V1	success or wait	16	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	12630	1176	00 00 00 04 fd fd fd fd 00 00 fd 00 fd 7b 57 77 38 17 18 01 00 00 00 00 00 00 18 01 fd 79 57 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 69 74 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 fd 7b 57 77 fd fd fd fd 00 00 00 00 00 00 4b 7f 00 00 00 00 30 07 4b 7f 00 00 5b 7f 28 02 5c 7f 50 06 5d 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 03 00 00 00 10 00 00 00 60 66 57 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 57 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 06 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	{Ww8yWwit{WwK0K[(\P]m `fWwPSWwB	success or wait	15	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	38102	256	2b 00 00 59 fd fd 75 13 fd fd 75 0f fd 7d 08 fd 74 09 fd 75 08 fd 2b 00 00 59 fd 4d fd 33 fd 5f fd 2b 00 00 fd fd 5d fd 55 fd fd 45 08 fd fd 21 fd 00 5d fd 55 fd fd fd 35 fd 21 fd 00 fd 15 0c fd fd 00 fd fd 74 03 5d fd fd fd 75 18 fd 75 14 fd 75 10 fd 75 0c fd 75 08 fd 11 00 00 00 fd 33 fd 50 50 50 50 50 fd fd fd fd fd fd fd 14 fd 6a 17 fd 14 fd 00 00 fd fd 74 05 6a 05 59 fd 29 56 6a 01 fd 17 04 00 fd 56 6a 02 fd 73 fd fd fd 56 fd 2a 00 00 fd fd 10 5e e1 04 41 fd 00 56 6a 14 5e fd fd 75 07 fd 00 02 00 00 fd 06 3b fd 7d 07 fd a3 04 41 fd 00 6a 04 50 fd fd 2e 00 00 fd 00 41 fd 00 59 59 fd fd 75 1e 6a 04 56 fd 35 04 41 fd 00 fd fd 2e 00 00 fd 00 41 fd 00 59 59 fd fd 75 05 6a 1a 58 5e fd 33 b9 10 10 fd 00 fd 0c 02 fd fd 20 fd 52 04 fd fd	+Yuu}tu+YM3_+]UE!]U5!t]uuuuu3PPPPPjtjY)VjVjsV*^AVj^u;}AjP.AYYujV5A.AYYujX^3R	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	1788	4	04 00 00 00		success or wait	4	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	9506	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 01 00 00 fd fd fd fd fd fd fd fd 4c fd fd 00 fd fd fd 00 23 00 00 00 02 02 00 00 34 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++L#4+	success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	1936	48	fd 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 60 fd 00 00 00 00 00 fd fd 5f 01 00 00 00 00 78 06 00 00 fd 75 00 00 fd 02 00 00 fd 2d 00 00	`_xu-	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	1996	4	2d 00 00 00	-	success or wait	45	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	7510	40	22 00 00 00 76 00 78 00 6d 00 74 00 62 00 6d 00 61 00 68 00 74 00 73 00 71 00 61 00 66 00 2e 00 65 00 78 00 65 00 00 00	"vxmtbmahtsqaf.exe	success or wait	45	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	6752	752	00 00 fd 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 3e 22 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 70 52 02 00 00 00 00 00 fd 0f 03 00 00 00 00 3f fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 28 03 00 00 00 00 00 73 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 24 14 00 00 00 00 00 fd fd 0b 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 0b 00 00 00 00	t`A!-a>"BB?#@AZbpR?s$@	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	38358	9070	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F88.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 00 13 00 00 fd 07 00 00 05 00 00 00 04 01 00 00 52 30 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 38 19 00 00 0c fd 00 00 15 00 00 00 fd 01 00 00 fd 1a 00 00 16 00 00 00 fd 00 00 00 fd 1c 00 00	R0T8T8	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6584</Pid>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1002	80	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 76 00 78 00 6d 00 74 00 62 00 6d 00 61 00 68 00 74 00 73 00 71 00 61 00 66 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>vxmtbmahtsqaf.exe</ImageName>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1082	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1086	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1090	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1180	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1184	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1188	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 39 00 34 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>20949</Uptime>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1232	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1236	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1240	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1322	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1326	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1330	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1382	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1386	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1390	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1434	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1438	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1444	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 35 00 34 00 30 00 34 00 32 00 32 00 31 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>540422144</PeakVirtualSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1532	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1536	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1542	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 35 00 34 00 30 00 34 00 31 00 38 00 30 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>540418048</VirtualSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1624	78	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 32 00 31 00 30 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>112103</PageFaultCount>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1712	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 34 00 35 00 37 00 36 00 35 00 30 00 31 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>457650176</PeakWorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1822	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 34 00 35 00 37 00 36 00 35 00 30 00 31 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>457650176</WorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1906	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1910	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	1916	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 32 00 31 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 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>172136</QuotaPeakPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2030	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2034	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2040	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 31 00 31 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>171144</QuotaPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2138	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2142	2	09 00		success or wait	3	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2148	128	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 35 00 34 00 35 00 37 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>3545704</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2276	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2280	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2286	112	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 35 00 34 00 35 00 35 00 36 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>3545568</QuotaNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2398	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2402	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2408	80	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 32 00 36 00 33 00 32 00 35 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>452632576</PagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2488	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2492	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2498	96	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 32 00 36 00 33 00 36 00 36 00 37 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>452636672</PeakPagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2594	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2598	2	09 00		success or wait	3	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2604	76	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 32 00 36 00 33 00 32 00 35 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>452632576</PrivateUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2680	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2684	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2688	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2734	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2738	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2742	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2772	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2776	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2782	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2822	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2826	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2834	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2864	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2868	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2876	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2946	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2950	2	09 00		success or wait	4	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	2958	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3060	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 39 00 37 00 34 00 30 00 33 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>3974035</Uptime>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3108	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3112	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3120	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3198	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3202	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3210	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3274	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3318	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3322	2	09 00		success or wait	5	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3332	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3422	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3426	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3436	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3510	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3514	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3524	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 36 00 33 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>49633</PageFaultCount>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3600	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3604	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3614	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 35 00 32 00 30 00 31 00 36 00 36 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>105201664</PeakWorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3714	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3718	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3728	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 38 00 33 00 36 00 31 00 33 00 34 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>98361344</WorkingSetSize>	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3810	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3814	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3824	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 35 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>96537 6</QuotaPeakPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3938	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3942	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	3952	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 39 00 38 00 32 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 >929824</Q uotaPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4050	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4054	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4064	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 32 00 35 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>72 504</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4188	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4192	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4202	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 39 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>69920< /QuotaNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4310	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4314	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4324	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 37 00 30 00 38 00 32 00 38 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>29708288</PagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4402	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4406	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4416	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 39 00 30 00 39 00 36 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>35909632</PeakPagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4510	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4514	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4524	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 37 00 30 00 38 00 32 00 38 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>29708288</PrivateUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4598	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4602	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4610	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4656	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4660	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4666	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4716	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4748	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4752	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4754	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4802	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4840	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4844	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4848	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4900	4	0d 00 0a 00		success or wait	9	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4904	2	09 00		success or wait	18	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	4908	84	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 76 00 78 00 6d 00 74 00 62 00 6d 00 61 00 68 00 74 00 73 00 71 00 61 00 66 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>vxmtbmahtsqaf.exe</Parameter0>	success or wait	9	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	5598	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	5602	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	5604	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	5644	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	5648	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	5650	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	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	5688	4	0d 00 0a 00		success or wait	6	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	5692	2	09 00		success or wait	12	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	5696	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6250	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6254	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6256	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6296	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6300	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6302	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6340	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6344	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6348	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6442	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6446	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6450	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 72 00 79 00 6d 00 69 00 61 00 64 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>rymiad, Inc.</SystemManufacturer>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6556	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6560	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6564	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 72 00 79 00 6d 00 69 00 61 00 64 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>rymiad7,1</SystemProductName>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6660	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6664	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6668	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6788	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6792	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6796	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 33 00 34 00 30 00 36 00 34 00 34 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>1603406440</OSInstallDate>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6878	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6882	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6886	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6988	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6992	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	6996	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7064	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7068	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7070	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7110	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7114	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7116	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7150	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7154	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7158	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7254	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7258	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7260	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7296	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7300	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7302	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7326	4	0d 00 0a 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7330	2	09 00		success or wait	6	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7334	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>80000000</Flags>	success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7586	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7590	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7618	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7622	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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 32 00 37 00 54 00 31 00 39 00 3a 00 31 00 33 00 3a 00 35 00 35 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-27T19:13:55Z">	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7724	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7728	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7732	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 35 00 38 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 37 00 38 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 37 00 38 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="400" PID="6584" UptimeMS="781" TimeSinceCreationMS="781" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7990	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	7994	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	8018	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	8022	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	8062	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	8066	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	8106	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	8110	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	8114	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 36 00 35 00 65 00 62 00 31 00 61 00 62 00 2d 00 38 00 62 00 34 00 64 00 2d 00 34 00 61 00 65 00 31 00 2d 00 39 00 35 00 62 00 33 00 2d 00 63 00 34 00 30 00 37 00 33 00 37 00 34 00 37 00 31 00 37 00 62 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>e65eb1ab-8b4d-4ae1-95b3-c407374717bb</Guid>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	8212	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	8216	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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 32 00 37 00 54 00 31 00 39 00 3a 00 31 00 33 00 3a 00 35 00 35 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-27T19:13:55Z</CreationTime>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	8318	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	8322	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.tmp.WERInternalMetadata.xml	8364	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA536.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	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA19.tmp.xml	0	4685	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vxmtbmahtsqaf.ex_cb9e76617add17783445895d2c3df37ac7ad2b_79937427_1794bb3d\Report.wer	0	2	fd fd		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vxmtbmahtsqaf.ex_cb9e76617add17783445895d2c3df37ac7ad2b_79937427_1794bb3d\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	172	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vxmtbmahtsqaf.ex_cb9e76617add17783445895d2c3df37ac7ad2b_79937427_1794bb3d\Report.wer	11772	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 35 00 37 00 39 00 34 00 31 00 33 00 36 00 37 00 38 00	MetadataHash=1579413678	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: WerFault.exe PID: **3976**, Parent PID: **6776**

General

Target ID:	19
Start time:	12:14:01
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6776 -s 176
Imagebase:	0xa20000
File size:	434592 bytes

MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
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	6DBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC745.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC745.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vxmtbmahtsqaf.ex_cb9e76617add17783445895d2c3df37ac7ad2b_79937427_0fb4cdeb	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vxmtbmahtsqaf.ex_cb9e76617add17783445895d2c3df37ac7ad2b_79937427_0fb4cdeb\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC745.tmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC745.tmp.xml	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6175.tmp.csv	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6186.tmp.txt	success or wait	1	6DBD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 22 fd 62 fd 05 12 00 00 00 00 00	MDMP "b	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.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 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 78 1a 00 00 fd 22 fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 20 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	UBGenuineIntelWTx"b Pacific Standard TimePacific Daylight Time	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	8606	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 fd 1e 00 00 fd 01 00 00 05 00 00 00 01 00 00 00 38 fd fd 00 fd fd fd 00 23 00 00 00 02 02 00 00 20 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++8# +	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	1620	168	7c 1a 00 00 00 00 00 00 09 04 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 00 00 00 00 00 01 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 21 00 00	|!	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	11470	20	0d 00 00 00 30 fd 3c 01 00 00 00 00 fd 04 00 00 fd 2d 00 00	0<-	success or wait	13	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	11682	1232	fd fd 4c 77 fd fd 4a 77 fd 00 00 00 fd fd fd fd 10 00 00 00 fd fd 3c 01 fd fd 3c 01 fd fd fd fd 40 fd 4a 77 40 fd 4a 77 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 50 fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 52 fd 00 fd fd 2c 01 78 30 00 01 fd fd 2c 01 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	LwJw<<@Jw@JwPTR,x0,	success or wait	12	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	29746	4	fd fd 2c 01	,	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	9322	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 01 00 00 fd fd fd fd fd fd fd 38 fd fd 00 fd fd fd 00 23 00 00 00 02 02 00 00 20 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++8# +	success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	1888	48	fd 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 30 fd 3c 01 00 00 00 00 fd 04 00 00 fd 2d 00 00 fd 02 00 00 02 2a 00 00	0<-*	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	7354	40	22 00 00 00 76 00 78 00 6d 00 74 00 62 00 6d 00 61 00 68 00 74 00 73 00 71 00 61 00 66 00 2e 00 65 00 78 00 65 00 00 00	"vxmtbmahtsqaf.exe	success or wait	44	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	6596	752	00 00 fd 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 50 5f 02 00 00 00 00 00 fd 0f 03 00 00 00 00 44 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 74 fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 5b fd 15 00 00 00 00 00 fd 2e 0a 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 09 0c 00 00 00 00	t`A!-a!BB? #@AZbP_Dt[.@	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	29750	8790	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0CB.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 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 20 18 00 00 6c 7e 00 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8T l~0	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6776</Pid>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1002	80	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 76 00 78 00 6d 00 74 00 62 00 6d 00 61 00 68 00 74 00 73 00 71 00 61 00 66 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>vxmtbmahtsqaf.exe</ImageName>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1082	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1086	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1090	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>000 00000</Cm dLineSignature>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1180	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1184	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1188	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 31 00 30 00 35 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>21059</Uptime>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1232	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1236	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1240	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1322	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1326	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1330	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1382	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1386	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1390	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1434	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1438	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1444	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 35 00 33 00 38 00 34 00 36 00 38 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>538468352</PeakVirtualSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1532	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1536	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1542	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 35 00 33 00 38 00 34 00 36 00 34 00 32 00 35 00 36 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>538464256</VirtualSize>	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1624	78	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 31 00 39 00 36 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>111967</PageFaultCount>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1712	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 34 00 35 00 37 00 32 00 33 00 36 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>457236480</PeakWorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1822	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 34 00 35 00 37 00 32 00 33 00 36 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>457236480</WorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1906	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1910	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	1916	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 30 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>170880</QuotaPeakPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2030	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2034	2	09 00		success or wait	3	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2040	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 36 00 39 00 38 00 38 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>169888</QuotaPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2138	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2142	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2148	128	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 35 00 34 00 34 00 35 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>3544592</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2276	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2280	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2286	112	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 35 00 34 00 34 00 34 00 34 00 35 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>3544456</QuotaNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2398	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2402	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2408	80	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 32 00 35 00 30 00 35 00 36 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>452505600</PagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2488	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2492	2	09 00		success or wait	3	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2498	96	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 32 00 35 00 30 00 39 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>452509696</PeakPagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2594	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2598	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2604	76	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 32 00 35 00 30 00 35 00 36 00 30 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>452505600</PrivateUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2680	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2684	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2688	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2734	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2738	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2742	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2772	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2776	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2782	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2822	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2826	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2834	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2864	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2868	2	09 00		success or wait	4	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2876	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2946	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2950	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	2958	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3060	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 39 00 38 00 32 00 34 00 30 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>3982400</Uptime>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3108	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3112	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3120	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3198	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3202	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3210	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3274	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	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3318	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3322	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3332	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3422	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3426	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3436	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3510	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3514	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3524	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 35 00 31 00 33 00 35 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>51358</PageFaultCount>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3600	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3604	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3614	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 35 00 32 00 30 00 31 00 36 00 36 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>105201664</PeakWorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3714	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3718	2	09 00		success or wait	5	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3728	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 34 00 39 00 37 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>104976384</WorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3812	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3816	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3826	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 35 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>965376</QuotaPeakPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3940	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3944	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	3954	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 34 00 34 00 30 00 34 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>944040</QuotaPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4052	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4056	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4066	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 33 00 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>73152</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4190	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4194	2	09 00		success or wait	5	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4204	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 37 00 33 00 30 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>73016</QuotaNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4312	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4316	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4326	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 35 00 32 00 33 00 33 00 37 00 39 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>352337 92</PagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4404	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4408	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4418	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 39 00 30 00 39 00 36 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>35 909632</P eakPagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4526	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 35 00 32 00 33 00 33 00 37 00 39 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>3523379 2</PrivateUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4600	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4604	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4612	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4668	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4718	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4756	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4798	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4802	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4804	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4842	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4846	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4850	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4902	4	0d 00 0a 00		success or wait	9	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4906	2	09 00		success or wait	18	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	4910	84	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 76 00 78 00 6d 00 74 00 62 00 6d 00 61 00 68 00 74 00 73 00 71 00 61 00 66 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>vxmtbmahtsqaf.exe</Parameter0>	success or wait	9	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	5600	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	5604	2	09 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	5606	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	5646	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	5650	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	5652	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	5690	4	0d 00 0a 00		success or wait	6	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	5694	2	09 00		success or wait	12	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	5698	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6252	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6256	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6258	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6298	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6302	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6304	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6342	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6346	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6350	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6444	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6448	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6452	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 72 00 79 00 6d 00 69 00 61 00 64 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>rymiad, Inc.</SystemManufacturer>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6558	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6562	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6566	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 72 00 79 00 6d 00 69 00 61 00 64 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>rymiad7,1</SystemProductName>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6662	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6666	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6670	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6790	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6794	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6798	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 33 00 34 00 30 00 36 00 34 00 34 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>1603406440</OSInstallDate>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6880	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6884	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6888	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	6998	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7066	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7070	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7072	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7112	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7116	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7118	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7152	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7156	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7160	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7256	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7260	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7262	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	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7298	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7302	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7304	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7328	4	0d 00 0a 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7332	2	09 00		success or wait	6	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7336	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>80000000</Flags>	success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7588	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7592	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7620	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7624	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.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 32 00 37 00 54 00 31 00 39 00 3a 00 31 00 34 00 3a 00 30 00 33 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-27T19:14:03Z">	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7726	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7730	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7734	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 37 00 37 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 37 00 39 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 37 00 39 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="404" PID="6776" UptimeMS="796" TimeSinceCreationMS="796" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7992	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	7996	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8000	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8020	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8024	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8026	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8064	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8068	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8070	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8108	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8112	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8116	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 33 00 62 00 63 00 35 00 64 00 37 00 61 00 2d 00 65 00 66 00 65 00 61 00 2d 00 34 00 64 00 36 00 62 00 2d 00 39 00 35 00 34 00 63 00 2d 00 31 00 33 00 32 00 36 00 32 00 61 00 63 00 33 00 64 00 35 00 33 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>83bc5d7a-efea-4d6b-954c-13262ac3d532</Guid>	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8214	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8218	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8222	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 32 00 37 00 54 00 31 00 39 00 3a 00 31 00 34 00 3a 00 30 00 33 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-27T19:14 :03Z</CreationTime>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8320	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8324	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8326	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8366	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC5BE.tmp.WERInternalMetadata.xml	8370	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC745.tmp.xml	0	4685	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vxmtbmahtsqaf.ex_cb9e76617add17783445895d2c3df37ac7ad2b_79937427_0fb4cdeb\Report.wer	0	2	fd fd		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vxmtbmahtsqaf.ex_cb9e76617add17783445895d2c3df37ac7ad2b_79937427_0fb4cdeb\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	171	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vxmtbmahtsqaf.ex_cb9e76617add17783445895d2c3df37ac7ad2b_79937427_0fb4cdeb\Report.wer	11672	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 32 00 34 00 39 00 38 00 31 00 33 00 31 00 30 00 30 00	MetadataHash=249813100	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly