

JoeSandbox Cloud BASIC



ID: 753418

Sample Name:

Ou0ZT4968y.exe

Cookbook: default.jbs

Time: 19:53:06

Date: 24/11/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report Ou0ZT4968y.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Sigma Signatures	3
Snort Signatures	4
Joe Sandbox Signatures	4
AV Detection	4
HIPS / PFW / Operating System Protection Evasion	4
Stealing of Sensitive Information	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
URLs from Memory and Binaries	7
World Map of Contacted IPs	7
General Information	7
Warnings	8
Simulations	8
Behavior and APIs	8
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASNs	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	9
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Ou0ZT4968y.exe_c69ec5e350e75532f4a4b55ffe3a71c9ab2f95_dac8cab9_132de5cf\Report.wer	99
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBEF.tmp.dmp	9
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDC28.tmp.WERInternalMetadata.xml	10
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDC5.tmp.xml	10
\Device\ConDrv	10
Static File Info	10
General	10
File Icon	11
Static PE Info	11
General	11
Entrypoint Preview	11
Data Directories	12
Sections	12
Imports	12
Network Behavior	13
Statistics	13
Behavior	13
System Behavior	13
Analysis Process: Ou0ZT4968y.exePID: 1308, Parent PID: 3528	13
General	13
File Activities	14
File Written	14
Analysis Process: conhost.exePID: 1236, Parent PID: 1308	14
General	14
Analysis Process: vbc.exePID: 60, Parent PID: 1308	14
General	14
File Activities	14
File Read	14
Analysis Process: WerFault.exePID: 4972, Parent PID: 1308	15
General	15
File Activities	15
File Created	15
File Deleted	15
File Written	16
Registry Activities	37
Key Created	37
Key Value Created	37
Disassembly	39

Windows Analysis Report

Ou0ZT4968y.exe

Overview

General Information

Sample Name:

Ou0ZT4968y.exe

Analysis ID:

753418

MD5:

27b75158dcfeba..

SHA1:

8a135c4fc3fa7e0..

SHA256:

a6ffd97ca5d47f2..

Tags:

32

exe

trojan

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

64

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

Writes to foreign memory regions

Allocates memory in foreign process...

Tries to harvest and steal browser in...

Injects a PE file into a foreign proce...

Uses 32bit PE files

One or more processes crash

Contains functionality to check if a d...

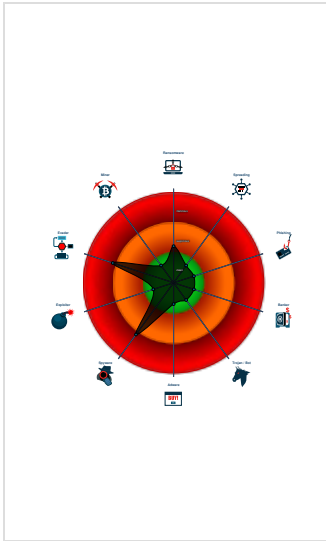
Contains functionality to query local...

Contains functionality to read the PE...

Uses code obfuscation techniques (...)

Checks if the current process is bei...

Classification



Process Tree

System is w10x64

Ou0ZT4968y.exe (PID: 1308 cmdline: C:\Users\user\Desktop\Ou0ZT4968y.exe MD5: 27B75158DCFEBAB3419BDBB15397584)

conhost.exe (PID: 1236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

vbc.exe (PID: 60 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)

WerFault.exe (PID: 4972 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1308 -s 192 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

cleanup

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Page 3 of 39

Snort Signatures

 No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

HIPS / PFW / Operating System Protection Evasion



Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

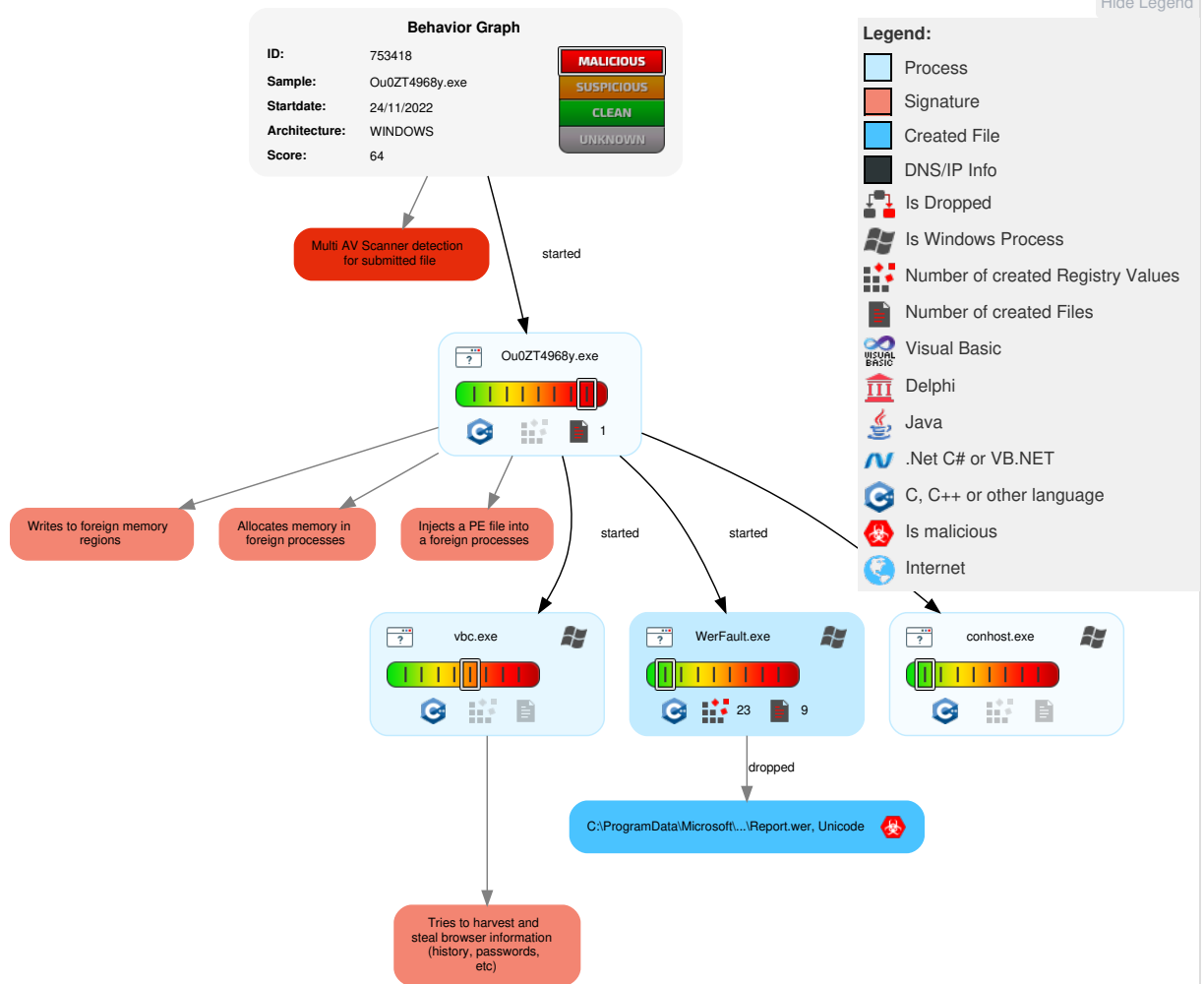


Tries to harvest and steal browser information (history, passwords, etc)

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	 Native API	Path Interception	 Process Injection	 Virtualization/Sandbox Evasion	 OS Credential Dumping	 System Time Discovery	Remote Services	 Archive Collected Data	Exfiltration Over Other Network Medium	 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	 Process Injection	LSASS Memory	 Security Software Discovery	Remote Desktop Protocol	 Data from Local System	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)	 Deobfuscate/Decode Files or Information	Security Account Manager	 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	 Obfuscated Files or Information	NTDS	 Remote System 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	 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
Ou0ZT4968y.exe	34%	Virustotal		Browse

Dropped Files

 No Antivirus matches

Unpacked PE Files

 No Antivirus matches

Domains

 No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://studio.youtube.comX-Originapplication/jsonContent-TypesessionTokenctx	0%	Avira URL Cloud	safe	
http://https://studio.youtube.comSAPISIDHASH	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	Ou0ZT4968y.exe, 00000000.00000000.330263752.0000000000CD3000.00000040.00000001.01000000.00000003.sdmp	false	URL Reputation: safe	unknown
http://https://gcc.gnu.org/bugs/):	Ou0ZT4968y.exe, 00000000.00000000.329876831.0000000000A6A000.00000004.00000001.01000000.00000003.sdmp	false		high
http://https://sectigo.com/CPS0	Ou0ZT4968y.exe, 00000000.00000000.330263752.0000000000CD3000.00000040.00000001.01000000.00000003.sdmp	false	URL Reputation: safe	unknown
http://https://studio.youtube.comSAPISIDHASH	Ou0ZT4968y.exe, 00000000.00000003.327858560.000000000163F000.00000040.00001000.00020000.00000000.sdmp, Ou0ZT4968y.exe, 00000000.00000000.329876831.0000000000A6A000.00000004.00000001.01000000.00000003.sdmp	false	Avira URL Cloud: safe	unknown
http://https://studio.youtube.comX-Originapplication/jsonContent-TypesessionTokenctx	Ou0ZT4968y.exe, 00000000.00000003.327858560.000000000163F000.00000040.00001000.00020000.00000000.sdmp, Ou0ZT4968y.exe, 00000000.00000000.329876831.0000000000A6A000.00000004.00000001.01000000.00000003.sdmp	false	Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	Ou0ZT4968y.exe, 00000000.00000000.330263752.0000000000CD3000.00000040.00000001.01000000.00000003.sdmp	false	URL Reputation: safe	unknown
http://https://studio.youtube.com	Ou0ZT4968y.exe, Ou0ZT4968y.exe, 00000000.00000003.327858560.000000000163F000.00000040.00001000.00020000.00000000.sdmp, Ou0ZT4968y.exe, 00000000.00000000.329876831.0000000000A6A000.00000004.00000001.01000000.00000003.sdmp	false		high
http://https://studio.youtube.com/reauth	Ou0ZT4968y.exe, Ou0ZT4968y.exe, 00000000.00000003.327858560.000000000163F000.00000040.00001000.00020000.00000000.sdmp, Ou0ZT4968y.exe, 00000000.00000000.329876831.0000000000A6A000.00000004.00000001.01000000.00000003.sdmp	false		high
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	Ou0ZT4968y.exe, 00000000.00000000.330263752.0000000000CD3000.00000040.00000001.01000000.00000003.sdmp	false	URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information	
Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753418
Start date and time:	2022-11-24 19:53:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ou0ZT4968y.exe

Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	10
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:	mal64.spyw.evad.winEXE@5/5@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 35% (good quality ratio 32.7%) • Quality average: 75.9% • Quality standard deviation: 29.7%
HCA Information:	• Successful, ratio: 58% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.20
- Excluded domains from analysis (whitelisted): login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus15.westus.cloudapp.azure.com, ctldl.windowsupdate.com, wa-tson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

 No simulations

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Ou0ZT4968y.exe_c69ec5e350e75532f4a4b55ffe3a71c9ab2f95_dac8cab9_132de5cf\

Report.wer 

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6329695668595557
Encrypted:	false
SSDEEP:	96:14IfvMywf97hool7RC6tpXlQcQvc6QcEDMcw3Dj+HbHg6ZAXGng5FMTPSkvPkpXf:ltBgCHBUZMXAjE/u7sYS274ltRd
MD5:	7AC4342A1B85811ABAC24B76E45FE49A
SHA1:	A8499CB46EECF8D8AC21AFDA6BE18035E241CB90
SHA-256:	8DCCCA9025CAD3C72E81F4F21E14D53A4E166B49F3888234D9447B8781ED2894
SHA-512:	2C6E21CBC1F723FB91C7568E4ECF3D84847CB06496A9A4ED7F248B246AA2767F717BA3F9CD133DD98E206D0B0542F21CDA8A14E4523DC8E6E38E2DF54409EC6B
Malicious:	true
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=1.....E.v.e.n.t.T.y.p.e.=B.E.X.....E.v.e.n.t.T.i.m.e.=1.3.3.1.3.7.8.9.6.5.4.1.8.9.4.3.1.0.....R.e.p.o.r.t.T.y.p.e.=2.....C.o.n.s.e.n.t.=1.....U.p.l.o.a.d.T.i.m.e.=1.3.3.1.3.7.8.9.6.5.5.8.9.2.5.5.3.3.....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.=5.0.e.3.a.d.b.6.-.1.2.9.4.-.4.1.0.c.-.9.7.2.9.-.d.b.c.c.4.b.7.9.7.c.1.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=1.0.a.6.1.a.a.2.-.9.c.7.2.-.4.0.c.c.-.a.6.a.1.-.d.3.2.3.3.6.d.b.8.2.8.9.....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.=O.u.0.Z.T.4.9.6.8.y...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.5.1.c.-.0.0.0.1.-.0.0.1.f.-.5.f.a.d.-.c.8.1.d.3.6.0.0.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=W.:0.0.0.6.0.b.5.3.c.e.d.0.4.4.c.0.0.7.6.6.b.3.c.0.8.7.f.d.b.8.c.c.b.7.a.0.0.0.0.f.f.f.f.0.0.0.0.8.a.1.3.5.c.4.f.c.3.f.a.7.e.0.6.b.f.2.9.5.3.7.f.9.c.b.0.2.9.8.c.c.2.f.1.c.1.d.e.!.O.u.0.Z.T.4.9.6.8.y...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=2.

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Nov 24 18:54:14 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	19652
Entropy (8bit):	2.034014938714263
Encrypted:	false
SSDEEP:	192:qlilum2KphOROi+6pLPZzJzd6C/EDfYv:snE0PZzJzdz
MD5:	D6CBDA626C8A5B9F30BF23C4A5174EAB
SHA1:	95C4B8E3290F8694C9FC7CC7A5501DB590A21579
SHA-256:	08521C7778E80CF397D6E9639DB800C4E9FDDC844263BAC6FC2418CC22A5F2EA
SHA-512:	E999E9DE6EEEC83F656EE68CE033773B25CC26C1806FE9A47056E149750B5EF4F8C592C9FCF28BB7C3598EDC8322065E22C207688A940B62F48AF30C932756
Malicious:	false
Reputation:	low
Preview:	MDMP.....c.....4.....<.....D.....T.....8.....T.....H...[C.....\.....H.....U.....B.....GenuineInt elW.....T.....c.....0.....W... .Eu.ro.pe. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .Eu.ro.pe. .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\WERCD28.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8420
Entropy (8bit):	3.6974458638675656
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNili6ldw/6YekSU5lgmfOSZGkV+prA89brrsFBZm:RrlsNiQ6ldw/6Y9SU5lgmfOSZGNrifu
MD5:	676E041CAED641FAA1D9F752A56D126D
SHA1:	799474AEAB27404D44C101393561B0C9BAED70BD
SHA-256:	C12A11E890F3AA61D532339AA79B37EF7A9B5BAE586B5063016AFB6E316466DA

SHA-512:	D75927353DF1DD3C797AE14B59D23F8A37F8C218E51D3CC042150347AB8E4C3A8C02AD50FF0E9D3AC9A7F8D9AE3C0FF16C43EDD98153CFE3C5F702B87C4DAE
Malicious:	false
Reputation:	low
Preview:	..<?.xm.l..v.e.r.s.i.o.n.="1...0"...e.n.c.o.d.i.n.g.="U.T.F.-1.6".?>.....<W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a>.....<O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n>.....<W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n>.1.0...0.</W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n>.....<B.u.i.l.d>.1.7.1.3.4.</B.u.i.l.d>.....<P.r.o.d.u.c.t>.(.0.x.3.0).;.W.i.n.d.o.w.s..1.0..P.r.o.</P.r.o.d.u.c.t>.....<E.d.i.t.i.o.n>.P.r.o.f.e.s.s.i.o.n.a.l.</E.d.i.t.i.o.n>.....<B.u.i.l.d.S.t.r.i.n.g>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4..r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</B.u.i.l.d.S.t.r.i.n.g>.....<R.e.v.i.s.i.o.n>.1.</R.e.v.i.s.i.o.n>.....<F.l.a.v.o.r>.M.u.l.t.i.p.r.o.c.e.s.s.o.r..F.r.e.e.</F.l.a.v.o.r>.....<A.r.c.h.i.t.e.c.t.u.r.e>.X.6.4.</A.r.c.h.i.t.e.c.t.u.r.e>.....<L.C.I.D>.1.0.3.3.</L.C.I.D>.....</O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n>.....<P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n>.....<P.i.d>.1.3.0.8.</P.i.d>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDC5.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4704
Entropy (8bit):	4.481568492896042
Encrypted:	false
SSDEEP:	48:cvlwSD8zsBJgtWI9HfWgc8sqYjD8fm8M4J2mLzMFt2+q8vFmLzFY+opNYzTd:uITfTAOgrsqY0J7zu2KSzy5pNYzTd
MD5:	FEF898BE98C3553564C2770855DD739C
SHA1:	32FEDBF10134E4B676D72E4784B9D59A8F275569
SHA-256:	18164DF80E19CD9DFDC743A86945DE336F3C0032E3BC1B5E745021462E87002D
SHA-512:	CDB02961084B4806FA5D7A49BD825997F86CFBBD0C3D8DE7F151854ED5D6066F3D34C98319ED71CA205C7F6B1CF58E352521119175AC79A56830D01DF0F98FD
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="1794484" />.. <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" />..

\Device\ConDrv	
Process:	C:\Users\user\Desktop\Ou0ZT4968y.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:E:E
MD5:	3C59DC048E8850243BE8079A5C74D079
SHA1:	472B07B9FCF2C2451E8781E944BF5F77CD8457C8
SHA-256:	6F4B6612125FB3A0DAECD2799DFD6C9C299424FD920F9B308110A2C1FBD8F443
SHA-512:	198DABF4BAC21CF35CDD848DB0F8B67C56B2BDF63767242AEA7342FE68C0B9DF8D37F3E47A134648E19F1640E158F2E527E636DB122A9143307CF309EFCB85D9
Malicious:	false
Reputation:	low
Preview:	21

Static File Info	
General	
File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	6.80554322520943
TrID:	- Win32 Executable (generic) a (10002005/4) 99.96% - 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:	Ou0ZT4968y.exe
File size:	3838464
MD5:	27b75158dcfeba6b3419bdbb15397584

SHA1:	8a135c4fc3fa7e06bf29537f9cb0298cc2f1c1de
SHA256:	a6ffd97ca5d47f2251a53ccd3ab891a9fec5b7d0f316b4c11e7d88f19765b1b4
SHA512:	eb9acc530d9c20dc26a00489572fe5b21075181f5f25d6598ebd5292aef5bbce9c2dc89fac04201ea7ce5c5faec545e44c02e54356ae6dfda7d2f70255a930b3
SSDEEP:	49152:Yl2A2+xup+pRTSHO1c6R7heQLqPqW7SdZ8iyTgyfw91m0tfSl8TtVlkQb9Hmv3IS:FneShqwhb/lkHv3lzT
TLSH:	B006CF710A5560CAE4D025F84AFB7772A7ECCBB02BC6C7CB428316A942D35C4A5B5F8D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....\$.K..*B..*B..AA..*B..AG..*B..AF..*B..AC..*B..C..*B..PF..*B..PA..*B..PG..*B..PG..*B..P@..*B..Rich.*B.....PE...L..

File Icon	
	
Icon Hash:	00828e8e8686b000

Static PE Info	
General	
Entrypoint:	0x4011b8
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x637FB129 [Thu Nov 24 18:00:09 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	a142061eae8e8b8626d2b5b074229afd

Entrypoint Preview	
Instruction	
jmp 00007EFE94CD4B0Fh	
jmp 00007EFE94CEB004h	
jmp 00007EFE94CDCE2Eh	
jmp 00007EFE94CC8254h	
jmp 00007EFE94CB01C7h	
jmp 00007EFE94D2D3EFh	
jmp 00007EFE94CC8985h	
jmp 00007EFE94CEB3A9h	
jmp 00007EFE94D33630h	
jmp 00007EFE94CB6385h	
jmp 00007EFE94CD52A7h	
jmp 00007EFE94CB4F2Ah	
jmp 00007EFE94CE5890h	
jmp 00007EFE94CBDB5Ch	
jmp 00007EFE94CFFD5Bh	
jmp 00007EFE94CB3ECFh	
jmp 00007EFE94CADE0Dh	
jmp 00007EFE94D20D01h	
jmp 00007EFE94CADEDCh	
jmp 00007EFE94CF9C19h	
jmp 00007EFE94CC518Eh	
jmp 00007EFE94CED845h	
jmp 00007EFE94CCFAEFh	

Instruction
jmp 00007EFE94CDDA06h
jmp 00007EFE94CB3861h
jmp 00007EFE94CF49F4h
jmp 00007EFE94D3024Bh
jmp 00007EFE94CEB8EFh
jmp 00007EFE94CBB9B9h
jmp 00007EFE94CD5E35h
jmp 00007EFE94CFFD21h
jmp 00007EFE94D298B8h
jmp 00007EFE94D19B74h
jmp 00007EFE94D127BDh
jmp 00007EFE94CBE12Dh
jmp 00007EFE94CDD920h
jmp 00007EFE94CECEF0h
jmp 00007EFE94CECED7h
jmp 00007EFE94CD3F1Dh
jmp 00007EFE94CCE109h

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x100	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3a41cc	0x28	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x100	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3a6000	0x47f4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb16a0	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xb15b8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3a4000	0x1cc	.idata
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	0x9ef24	0x9f000	False	0.3489721526139937	data	5.808660940243666	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xa0000	0x19ddc	0x19e00	False	0.3395889945652174	data	4.119191864178727	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.data	0xba000	0x2e9bc4	0x2e8000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x3a4000	0xbdb	0xc00	False	0.3610026041666667	data	4.663842800729639	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.00cfg	0x3a5000	0x10e	0x200	False	0.03515625	data	0.11055713125913882	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3a6000	0x71bd	0x7200	False	0.4772820723684211	data	4.965115122336909	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

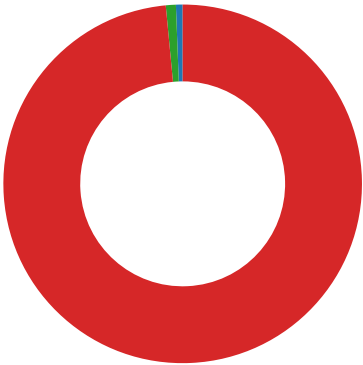
DLL	Import
KERNEL32.dll	FormatMessageA, WideCharToMultiByte, MultiByteToWideChar, GetStringTypeW, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionEx, DeleteCriticalSection, LocalFree, EncodePointer, DecodePointer, LCMAPStringEx, GetLocaleInfoEx, CompareStringEx, GetCPInfo, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, GetModuleHandleW, CreateFileW, RaiseException, RtlUnwind, InterlockedPushEntrySList, InterlockedFlushSList, GetLastError, SetLastError, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, GetStdHandle, WriteFile, GetModuleFileNameW, ExitProcess, GetModuleHandleExW, GetCommandLineA, GetCommandLineW, GetCurrentThread, HeapAlloc, HeapFree, GetFileType, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMAPStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, CloseHandle, FlushFileBuffers, GetConsoleOutputCP, GetConsoleMode, ReadFile, GetFileSizeEx, SetFilePointerEx, ReadConsoleW, HeapReAlloc, SetConsoleCtrlHandler, GetTimeZoneInformation, OutputDebugStringW, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableW, SetStdHandle, GetProcessHeap, HeapSize, WriteConsoleW

Network Behavior

 No network behavior found

Statistics

Behavior



- Ou0ZT4968y.exe
- conhost.exe
- vbc.exe
- WerFault.exe



Click to jump to process

System Behavior

Analysis Process: Ou0ZT4968y.exe PID: 1308, Parent PID: 3528

General

Target ID:	0
Start time:	19:54:01
Start date:	24/11/2022
Path:	C:\Users\user\Desktop\Ou0ZT4968y.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Ou0ZT4968y.exe
Imagebase:	0x9b0000
File size:	3838464 bytes
MD5 hash:	27B75158DCFEB6B3419BDBB15397584
Has elevated privileges:	true

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\\Device\\ConDrv	1	1	31	1	success or wait	2	A2ECB8	WriteFile
unknown	unknown	1			invalid handle	1	A2ECB8	WriteFile

Analysis Process: conhost.exe PID: 1236, Parent PID: 1308

General

Target ID:	1
Start time:	19:54:01
Start date:	24/11/2022
Path:	C:\\Windows\\System32\\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\\Windows\\system32\\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vbc.exe PID: 60, Parent PID: 1308

General

Target ID:	2
Start time:	19:54:11
Start date:	24/11/2022
Path:	C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\vbc.exe
Imagebase:	0x190000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\\Users\\user\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Network\\Cookies	0	100	success or wait	1	4AF6172	ReadFile
C:\\Users\\user\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Network\\Cookies	0	4096	success or wait	1	4AF6172	ReadFile
C:\\Users\\user\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Network\\Cookies	24	16	success or wait	1	4AF6172	ReadFile

Analysis Process: WerFault.exe PID: 4972, Parent PID: 1308

General

Target ID:	5
Start time:	19:54:13
Start date:	24/11/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1308 -s 192
Imagebase:	0xf40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D8E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBFE.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBFE.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDC5.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDC5.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Ou0ZT4968y.exe_c69ec5e350e75532f4a4b55ffe3a71c9ab2f95_dac8cab9_132de5cf	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Ou0ZT4968y.exe_c69ec5e350e75532f4a4b55ffe3a71c9ab2f95_dac8cab9_132de5cf\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D8D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBFE.tmp	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDC5.tmp	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBFE.tmp.dmp	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDC5.tmp.xml	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCE11.tmp.csv	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF3B.tmp.txt	success or wait	1	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBFE.tmp.dmp	15916	3736	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(WaitCompletionPa cketIoCo mpletionTpWorkerFactor yIRTimer (WaitCompletionPacketI RTimer(WaitCompl	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBFE.tmp.dmp	32	108	03 00 00 00 34 00 00 00 fd 06 00 00 04 00 00 00 20 02 00 00 3c 07 00 00 05 00 00 00 44 00 00 00 14 12 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 48 09 00 00 7c 43 00 00 15 00 00 00 fd 01 00 00 5c 09 00 00 16 00 00 00 fd 00 00 00 48 0b 00 00	4 <DT8TH C\H	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.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	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 33 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1308</Pid>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 4f 00 75 00 30 00 5a 00 54 00 34 00 39 00 36 00 38 00 79 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>Ou0ZT4968y.exe</ImageName>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1084	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1182	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 33 00 32 00 37 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>13279</Uptime>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1226	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1230	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1234	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1316	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1320	2	09 00		success or wait	2	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1324	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1376	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1380	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1384	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1428	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1432	2	09 00		success or wait	3	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1438	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 31 00 30 00 31 00 36 00 38 00 34 00 30 00 31 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>1016840192</PeakVirtualSize>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1528	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1532	2	09 00		success or wait	3	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1538	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 36 00 38 00 30 00 31 00 37 00 39 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>16801792</VirtualSize>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1608	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1612	2	09 00		success or wait	3	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1618	78	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 34 00 37 00 30 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>247064</PageFaultCount>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1696	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1700	2	09 00		success or wait	3	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1706	102	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 30 00 36 00 36 00 36 00 39 00 38 00 32 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>1006669824</PeakWorkingSetSize>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1808	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1812	2	09 00		success or wait	3	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1818	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 30 00 34 00 35 00 31 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7045120</WorkingSetSize>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1898	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1902	2	09 00		success or wait	3	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	1908	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 31 00 36 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>40160</QuotaPeakPagedPoolUsage>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2020	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2024	2	09 00		success or wait	3	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2030	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 38 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>31848</QuotaPagedPoolUsage>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2126	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2130	2	09 00		success or wait	3	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2136	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 34 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>28424</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2260	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2264	2	09 00		success or wait	3	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2270	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>28072</QuotaNonPagedPoolUsage>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2378	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2382	2	09 00		success or wait	3	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2388	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 32 00 39 00 30 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3629056</PagefileUsage>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2464	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2468	2	09 00		success or wait	3	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2474	98	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 30 00 35 00 35 00 37 00 36 00 31 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1005576192</PeakPagefileUsage>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2572	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2576	2	09 00		success or wait	3	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2582	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 32 00 39 00 30 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3629056 </PrivateUsage>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2654	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2658	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2662	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2708	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2712	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2716	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2746	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2750	2	09 00		success or wait	3	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2756	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2796	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2800	2	09 00		success or wait	4	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2808	30	3c 00 50 00 69 00 64 00 3e 00 33 00 35 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3528</Pid>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2838	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2842	2	09 00		success or wait	4	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2850	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2920	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2924	2	09 00		success or wait	4	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	2932	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3022	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3026	2	09 00		success or wait	4	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3034	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 33 00 31 00 32 00 30 00 33 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4312030</Uptime>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3082	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3086	2	09 00		success or wait	4	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3094	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3172	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3176	2	09 00		success or wait	4	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3184	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3236	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3240	2	09 00		success or wait	4	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3248	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3292	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3296	2	09 00		success or wait	5	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3306	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3396	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3400	2	09 00		success or wait	5	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3410	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3484	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3488	2	09 00		success or wait	5	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3498	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 38 00 38 00 31 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>58815</PageFaultCount>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3574	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3578	2	09 00		success or wait	5	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3588	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 32 00 30 00 38 00 37 00 32 00 39 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>120872960</PeakWorkingSetSize>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3688	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3692	2	09 00		success or wait	5	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3702	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 32 00 30 00 33 00 34 00 34 00 35 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>120344576</WorkingSetSize>	success or wait	1	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3786	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3790	2	09 00		success or wait	5	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3800	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 33 00 35 00 30 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>1135040</QuotaPeakPagedPoolUsage>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3916	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3920	2	09 00		success or wait	5	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	3930	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 39 00 33 00 30 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>1093088</QuotaPagedPoolUsage>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4030	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4034	2	09 00		success or wait	5	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4044	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 37 00 36 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>87600</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4168	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4172	2	09 00		success or wait	5	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4182	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 32 00 30 00 38 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>82080</QuotaNonPagedPoolUsage>	success or wait	1	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4290	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4294	2	09 00		success or wait	5	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4304	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 33 00 37 00 36 00 35 00 37 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>43765760</PagefileUsage>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4382	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4386	2	09 00		success or wait	5	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4396	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 34 00 31 00 36 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>45416448</PeakPagefileUsage>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4490	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4494	2	09 00		success or wait	5	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4504	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 33 00 37 00 36 00 35 00 37 00 36 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>43765760</PrivateUsage>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4578	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4582	2	09 00		success or wait	4	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4590	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4636	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4640	2	09 00		success or wait	3	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4646	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4688	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4692	2	09 00		success or wait	2	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4696	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4728	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4732	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4734	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4776	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4780	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4782	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4820	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4824	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4828	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4880	4	0d 00 0a 00		success or wait	9	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4884	2	09 00		success or wait	18	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	4888	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 4f 00 75 00 30 00 5a 00 54 00 34 00 39 00 36 00 38 00 79 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>Ou0ZT4968y.exe</Parameter0>	success or wait	9	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	5606	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	5610	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	5612	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	5652	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	5656	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	5658	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	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	5696	4	0d 00 0a 00		success or wait	6	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	5700	2	09 00		success or wait	12	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	5704	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>10.0.17134.2.0.0.2 56.48</Parameter1>	success or wait	6	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6258	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6262	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6264	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6304	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6308	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6310	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6348	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6352	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6356	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6450	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6454	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6458	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 67 00 6e 00 72 00 74 00 69 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>gnrtid, Inc. </SystemManufacturer>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6564	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6568	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6572	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 67 00 6e 00 72 00 74 00 69 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>gnrtid7,1</SystemProductName>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6668	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6672	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6676	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6796	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6800	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6804	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 32 00 32 00 38 00 32 00 32 00 38 00 36 00 33 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>1622822863</OSInstallDate>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6886	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6890	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6894	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	2	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7004	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7074	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7078	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7080	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7120	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7124	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7126	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7160	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7164	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7168	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	<UEFI SecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7264	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7268	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7270	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7306	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7310	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7312	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7336	4	0d 00 0a 00		success or wait	3	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7340	2	09 00		success or wait	6	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7344	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags> >	success or wait	3	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7590	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7594	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7596	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7622	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7626	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7628	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 31 00 31 00 2d 00 32 00 34 00 54 00 31 00 38 00 3a 00 35 00 34 00 3a 00 31 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11- 24T18:54:14Z">	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7728	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7732	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	7736	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 32 00 39 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 33 00 30 00 38 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 31 00 30 00 38 00 39 00 30 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 31 00 30 00 38 00 39 00 30 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<Process AsId="292" PID="1308" UptimeMS="10890" TimeSinceCreationMS="10890" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8002	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8006	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8010	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	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8030	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8034	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8036	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8074	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8078	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8080	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8118	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8122	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8126	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 30 00 65 00 33 00 61 00 64 00 62 00 36 00 2d 00 31 00 32 00 39 00 34 00 2d 00 34 00 31 00 30 00 63 00 2d 00 39 00 37 00 32 00 39 00 2d 00 64 00 62 00 63 00 63 00 34 00 62 00 37 00 39 00 37 00 63 00 31 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>50e3adb6-1294-410c-9729-dbcc4b797c1f</Guid>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8224	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8228	2	09 00		success or wait	2	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8232	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 31 00 31 00 2d 00 32 00 34 00 54 00 31 00 38 00 3a 00 35 00 34 00 3a 00 31 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-11-24T18:54:14Z</CreationTime>	success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8330	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8334	2	09 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8336	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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8376	4	0d 00 0a 00		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD28.tmp.WERInternalMetadata.xml	8380	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	6D8D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDC5.tmp.xml	0	4704	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 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	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Ou0ZT4968y.exe_c69ec5e350e75532f4a4b55ffe3a71c9ab2f95_dac8cab9_132de5cf\Report.wer	0	2	fd fd		success or wait	1	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Ou0ZT4968y.exe_c69ec5e350e75532f4a4b55ffe3a71c9ab2f95_dac8cab9_132de5cf\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	132	6D8D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Ou0ZT4968y.exe_c69ec5e350e75532f4a4b55ffe3a71c9ab2f95_dac8cab9_132de5cf\Report.wer	7456	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 39 00 30 00 38 00 31 00 30 00 31 00 33 00 30 00 31 00	MetadataHash=90810130 1	success or wait	1	6D8D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities						
Key Created						
Key Path			Completion	Count	Source Address	Symbol
\REGISTRY\A\{31b051f3-a409-8ac3-1822-529041218f7e}\Root\InventoryApplicationFile\PermissionsCheckTestKey			success or wait	1	6D8F36BF	unknown
\REGISTRY\A\{31b051f3-a409-8ac3-1822-529041218f7e}\Root\InventoryApplicationFile\PermissionsCheckTestKey			success or wait	1	6D8F36BF	unknown
\REGISTRY\A\{31b051f3-a409-8ac3-1822-529041218f7e}\Root\InventoryApplicationFile\ou0zt4968y.exe\86d131a8			success or wait	1	6D8F36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug			success or wait	1	6D8F1FB2	RegCreateKeyExW
\REGISTRY\A\{31b051f3-a409-8ac3-1822-529041218f7e}\Root\InventoryApplicationFile\PermissionsCheckTestKey			success or wait	1	6D8D43D1	unknown

Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{31b051f3-a409-8ac3-1822-529041218f7e}\Root\InventoryApplicationFile\ou0zt4968y.exe\86d131a8	ProgramId	unicode	00060b53ced0444c00766b3c087fdb8ccb7a0000ffff	success or wait	1	6D8F36BF	unknown
\REGISTRY\A\{31b051f3-a409-8ac3-1822-529041218f7e}\Root\InventoryApplicationFile\ou0zt4968y.exe\86d131a8	FileId	unicode	00008a135c4fc3fa7e06bf29537f9cb0298cc2f1c1de	success or wait	1	6D8F36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	LowerCaseLongPath	unicode	c:\\users\\user\\desktop\\ou0zt4968y.exe	success or wait	1	6D8F36BF	unknown
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	LongPathHash	unicode	ou0zt4968y.exe\\86d131a8	success or wait	1	6D8F36BF	unknown
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	Name	unicode	ou0zt4968y.exe	success or wait	1	6D8F36BF	unknown
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	Publisher	unicode		success or wait	1	6D8F36BF	unknown
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	Version	unicode		success or wait	1	6D8F36BF	unknown
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	BinFileVersion	unicode		success or wait	1	6D8F36BF	unknown
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	BinaryType	unicode	pe32_!386	success or wait	1	6D8F36BF	unknown
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	ProductName	unicode		success or wait	1	6D8F36BF	unknown
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	ProductVersion	unicode		success or wait	1	6D8F36BF	unknown
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	LinkDate	unicode	11/24/2022 18:00:09	success or wait	1	6D8F36BF	unknown
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	BinProductVersion	unicode		success or wait	1	6D8F36BF	unknown
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	Size	B	00 92 3A 00 00 00 00 00	success or wait	1	6D8F36BF	unknown
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	Language	dword	0	success or wait	1	6D8F36BF	unknown
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	IsPeFile	dword	1	success or wait	1	6D8F36BF	unknown
\\REGISTRY\\A\\{31b051f3-a409-8ac3-1822-529041218f7e}\\Root\\InventoryApplicationFile\\ou0zt4968y.exe\\86d131a8	IsOsComponent	dword	0	success or wait	1	6D8F36BF	unknown

