ID: 882710
Sample Name: file.exe
Cookbook: default.jbs
Time: 17:21:07
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

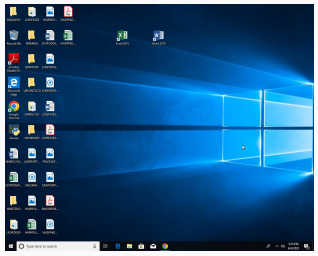
Windows Analysis Report

file.exe

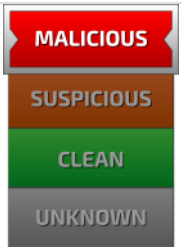
Overview

General Information

Sample Name:	file.exe
Analysis ID:	882710
MD5:	296fd972f13fe3..
SHA1:	056a3fbe0a88a..
SHA256:	7f6453437b84c..
Tags:	NET exe MSIL
Infos:	



Detection



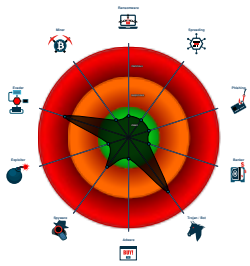
BlackGuard

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Yara detected BlackGuard
- Multi AV Scanner detection for subm…
- .NET source code contains very larg…
- Yara detected Costura Assembly Lo…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Uses 32bit PE files
- AV process strings found (often use…
- Queries the volume information (nam…
- Sample file is different than original …

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 3360 cmdline: C:\Users\user\Desktop\file.exe MD5: 296FD972F13FE3F371D16FF2430A3E81)
  - WerFault.exe (PID: 5956 cmdline: C:\Windows\system32\WerFault.exe -u -p 3360 -s 944 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
BlackGuard	According to Zscaler, BlackGuard has the capability to steal all types of information related to Crypto wallets, VPN, Messengers, FTP credentials, saved browser credentials, and email clients.	No Attribution	**http://** https://blog.cyble.com/2022/04/01/dissecting-blackguard-info-stealer/https://blogs.blackberry.com/en/2022/04/threat-thursday-blackguard-infostealerhttps://cyberint.com/blog/research/blackguard-stealer/https://ke-la.com/information-stealers-a-new-landscape/https://medium.com/s2wblog/rising-stealer-in-q1-2022-blackguard-stealer-f516d9f85ee5	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.blackguard

Malware Configuration

Threatname: BlackGuard

```
{
  "C2 url": "http://94.142.138.111"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.410785101.0000000013EBC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000000.00000002.410785101.0000000013EBC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_BlackGuard	Yara detected BlackGuard	Joe Security	
00000000.00000002.410785101.0000000013EBC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.414643984.000000001BC10000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000000.00000002.414643984.000000001BC10000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_BlackGuard	Yara detected BlackGuard	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.file.exe.13ebcb40.2.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0.2.file.exe.13ebcb40.2.unpack	JoeSecurity_BlackGuard	Yara detected BlackGuard	Joe Security	
0.2.file.exe.13ebcb40.2.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.2.file.exe.1bc10000.3.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0.2.file.exe.1bc10000.3.unpack	JoeSecurity_BlackGuard	Yara detected BlackGuard	Joe Security	
Click to see the 13 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Found malware configuration

Yara detected BlackGuard

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

E-Banking Fraud

Yara detected BlackGuard

System Summary

.NET source code contains very large array initializations

Data Obfuscation

Yara detected Costura Assembly Loader

.NET source code contains potential unpacker

Stealing of Sensitive Information

Yara detected BlackGuard

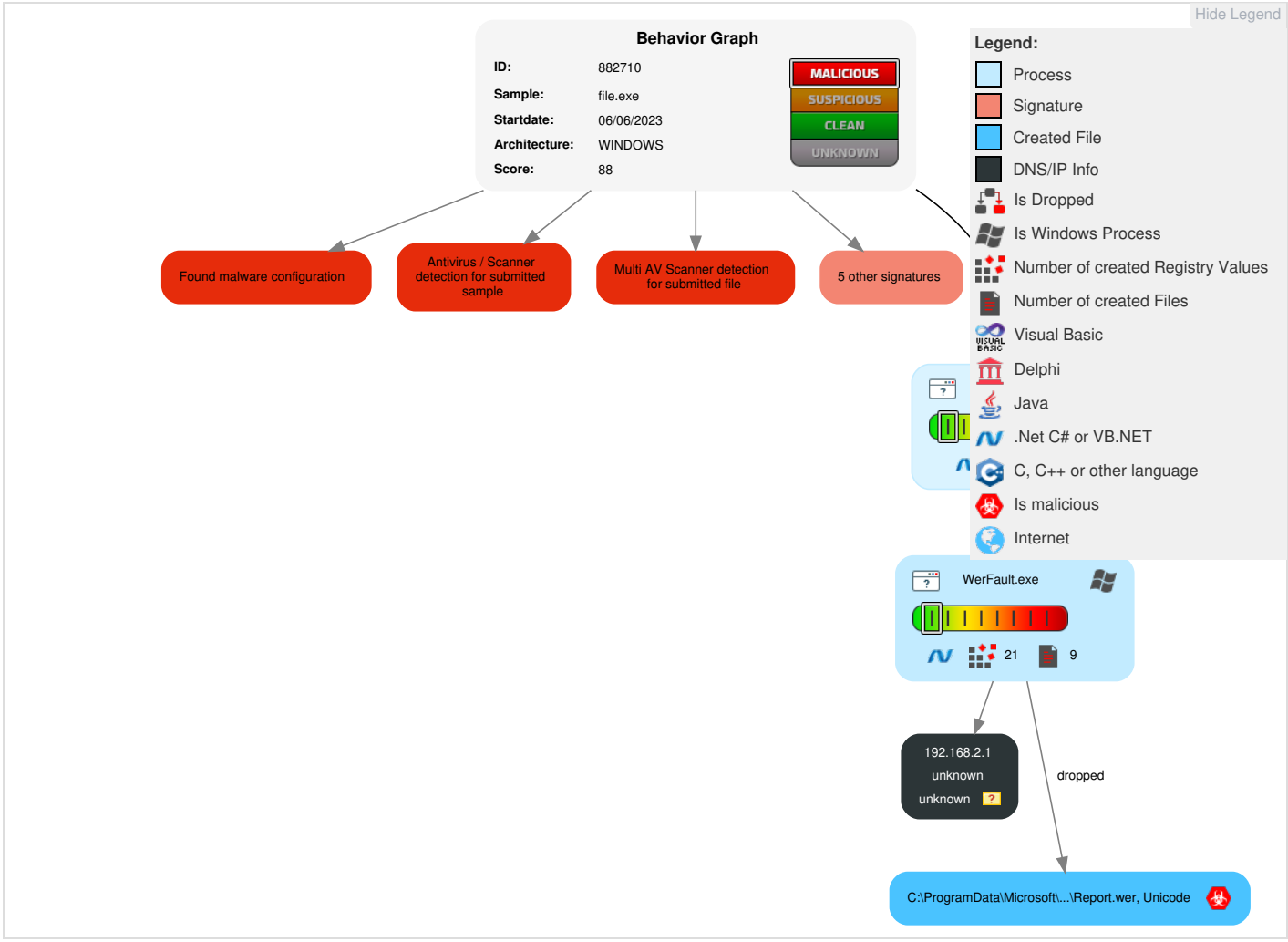
Remote Access Functionality

Yara detected BlackGuard

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	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Virtualization/Sandbox Evasion	OS Credential Dumping	2 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	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	1 Disable or Modify Tools	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Software Packing	Security Account Manager	1 2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

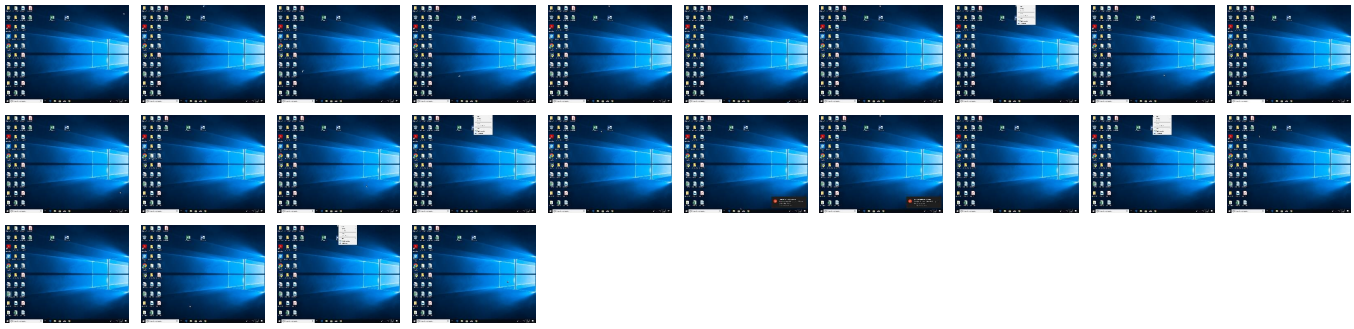
Behavior Graph



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
file.exe	32%	ReversingLabs	ByteCode-MSIL.Packed.Generic	
file.exe	46%	Virustotal		Browse
file.exe	100%	Avira	HEUR/AGEN.1311119	
file.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://upx.sf.net	Amcache.hve.3.dr	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882710
Start date and time:	2023-06-06 17:21:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	8
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
Sample file name:	file.exe
Detection:	MAL
Classification:	mal88.troj.evad.winEXE@2/5@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.168.117.173
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, ctldl.windowsupdate.com, watson.telemetry.microsoft.com
- Execution Graph export aborted for target file.exe, PID 3360 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:22:11	API Interceptor	2x Sleep call for process: file.exe modified
17:22:25	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_d2892c472895a2b98efdcdcd7642ab4d7ea6c2_3b20dbdc_17059a9d\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.0154175955898803
Encrypted:	false
SSDEEP:	192:FaBDbqevl2/NHJivpxIxa1ukczu/u7s1S274ltoB:2DbDoJivpoackh/u7s1X4ltc
MD5:	5D7C9AA3EEF5CC7D1ABB8FFB78C3FECB
SHA1:	F7049D063B2313BB3F38E13F60B1C014628F14D2
SHA-256:	2BC6CE33C528A5B6195C2D819AB4393D3A7A3044307E28F1C60143985ADBC10F
SHA-512:	F44882EBFC915880146CEA2D1F4BB8BF9FFCAA61D385D87B11E0E77148D444FAE84791E18E640FF51A9267C396645FCE8B2D0ACE84E57F245D60526879F811D
Malicious:	**true**
Reputation:	low

Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.7.0.9.3.7.6.2.9.6.2.1.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.7.0.9.3.8.4.8.8.9.5.0.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.5.d.6.a.0.3.d.-.1.2.2.c.-.4.8.8.3.-.9.9.8.8.-.e.a.7.6.3.6.c.e.b.3.7.a.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.6.c.2.2.a.9.c.-.c.5.c.6.-.4.c.0.c.-.8.5.5.5.-.9.2.d.9.9.1.6.9.d.3.4.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.f.i.l.e...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.P.y.t.h.o.n. .C.o.n.s.o.l.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.d.2.0.-.0.0.0.1.-.0.0.1.f.-.f.9.1.5.-.c.1.1.6.d.6.9.8.d.9.0.1...T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.6.b.3.3.f.2.f.1.3.c.1.6.5.3.8.3.0.2.c.a.6.8.1.b.f.7.1.4.0.6.9.4.0.0.0.0.0.0.0.0.0.!.0.0.0.0.0.5.6.a.3.f.b.e.0.a.8.8.a.3.9.3.4.8.e.8.b.9.9.f.0.c.f.f.b.3.c.6.e.6.3.b.5.6.5.5.!.f.i.l.e...e.x.e.....T.a.r.g.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed Jun 7 00:22:17 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	289968
Entropy (8bit):	3.3909347167244874
Encrypted:	false
SSDEEP:	3072:il9tolbqg5YuGUF0+EEShwv5XtS94hLPZkl9c4s:ebObqSBYhYdSwPZW
MD5:	81845BC11C970609E81A250C871F402B
SHA1:	29F03795D3E282977C3393FDF4847080F68D3BA3
SHA-256:	DD047031CA85FFEA7129EFC5A4BFFCA8BEA1BD28315EC10EC382CD216B9473A8
SHA-512:	DD0B95F708FA19F7FFE6BF89B7A2FAA79648A85ABCF5BB5EDDCE6AAF3CE4A96BF0FA1BDB211858BBC99125E642F99AAD27B123C1472A3861AE9A1CD2E67BE981
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....d.....$.....8.....D....I.....`.....8.....T.....@%..pG.....I.....U.....B.....("...Lw.....`.....T..... .....d.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...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.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8816
Entropy (8bit):	3.70405814562524
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiCCeZ+6YqgBQgmfZDLeSUpCprr89bpb+hfjDm:RrlsNiog6Yt2gmf0SUdpbof2
MD5:	FB7B29A54D8CF8060A2DF2713E668E59
SHA1:	58190D23054A48AD969A89DE13EAA6DF8970FA7B
SHA-256:	285CF8C1B2948009E7BE858FB0D0B0A274D340CEEB4E6FB919E28E1D23E84B75
SHA-512:	DF967CA532966182155694A2D23319B644C6526F1C76AA81EAB531B5C9142E8E95A06E4F8FF7DB974B07D588DDC564C30828E4705DAF75A7AC305FF8FAFEF98
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.3.6.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E4D.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4781
Entropy (8bit):	4.481383546237062
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtBl9XXWgc8sqYjQ8fm8M4JFXFzQyq8vx9eUurGcTxkd:uITflNmgrsqYhJvQWneUjcTxkd
MD5:	E15867255930E0632D7C0E0D4784C21B
SHA1:	B64BD604EBE9D7AA4F9B9A75047E7B0FE4EEFF7F
SHA-256:	16822727642A0792854113C8A8D9D5759CC1ADA9A584DFFC340A4843D5388799
SHA-512:	4E4C9241161A7F33D458BAA0F2DA1ECD17A7AC6E0A644727DE501A9217595BA00D7AC384313F65B8F50F982F31F21CCBD12203D48B02CA8075878D6DEC87035
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="2074172" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Windows\appcompat\Programs\Amcache.hve

Process:	C:\Windows\System32\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.286984272816522
Encrypted:	false
SSDEEP:	12288:v/jK0Th312aptTSP2C/doN515xzNu2R+GrNHk+DVl/lQG6bnv/OmaaoS:DK0Th312aptTSP+HL
MD5:	3D402A369D6390F9E65DE08D1DE8637F
SHA1:	62924C83353B75BB7A5D9B9DD38AFA62B390DB45
SHA-256:	24FC9B4DA4BA3FC4012009E644D029CD56EF645B9A40574438524D004AB7B3AE
SHA-512:	031F4853E87EA16820D9718A8B14F426480C9876975C8F3785FB7EF957552DCD39594BA3F5A2135554DF6E32AC49DF6D293FD776ACF4618E3D013B85A64C111B
Malicious:	false
Reputation:	low
Preview:	regfi...i...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm._. .....@. .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.9353492722044665
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	file.exe
File size:	3661312
MD5:	296fd972f13fe3f371d16ff2430a3e81
SHA1:	056a3fbe0a88a39348e8b99f0cffb3c6e63b5655
SHA256:	7f6453437b84cd7518a1e628565a13f76bf09aa376eab94224fc269e3ef804a5
SHA512:	35c8a54f60f440333bb282459eb4db7f62f5abfb4c16fa0655df8d5a434f66b49bbb7a49543741462f60439ee6bf8b2b9547b7241954e500687cc06bd226ccb1
SSDEEP:	98304:46UJZSh7kjoRtHOrpMsgD+TPzxpCQcYOi:pwQh7kjoihFTZOi
TLSH:	77063355A98690D4C4FE96394B778BF51B5E4E0374E6C24E33D4BB26C8BC084F9293A3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Id.....<5..<.....Z5.. ...`5...@.. .....6.....@.....

File Icon

Icon Hash:	196d763009651118

Static PE Info

General

Entrypoint:	0x755ade
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x646CB611 [Tue May 23 12:48:17 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x355a8c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x356000	0x138a0	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x36a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x353ae4	0x353c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x356000	0x138a0	0x13a00	False	0.49946506767515925	data	6.156042221592264	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x36a000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x356340	0x3d97	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x35a0d8	0x1628	Device independent bitmap graphic, 64 x 128 x 8, image size 4096, 256 important colors		
RT_ICON	0x35b700	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors		
RT_ICON	0x35c5a8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors		
RT_ICON	0x35ce50	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors		
RT_ICON	0x35d518	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors		
RT_ICON	0x35da80	0x30fa	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x360b7c	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896		
RT_ICON	0x364da4	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600		
RT_ICON	0x36734c	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224		
RT_ICON	0x3683f4	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400		
RT_ICON	0x368d7c	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088		
RT_GROUP_ICON	0x3691e4	0xae	data		
RT_VERSION	0x369294	0x420	data		
RT_MANIFEST	0x3696b4	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

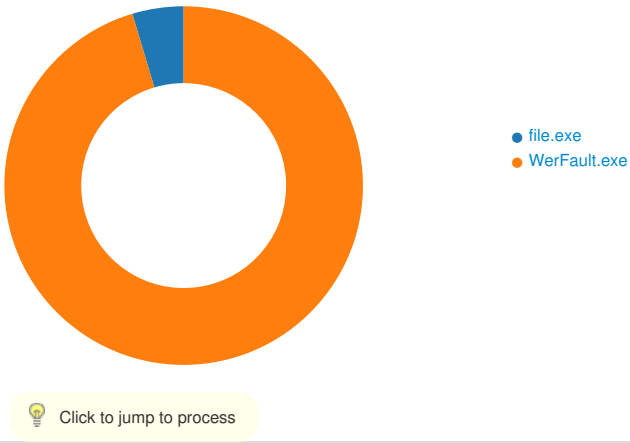
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 3360, Parent PID: 3452

General

Target ID:	0
Start time:	17:22:05
Start date:	06/06/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0xb00000
File size:	3661312 bytes
MD5 hash:	296FD972F13FE3F371D16FF2430A3E81
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.410785101.0000000013EBC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BlackGuard, Description: Yara detected BlackGuard, Source: 00000000.00000002.410785101.0000000013EBC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.410785101.0000000013EBC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.414643984.000000001BC10000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BlackGuard, Description: Yara detected BlackGuard, Source: 00000000.00000002.414643984.000000001BC10000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.414643984.000000001BC10000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.410785101.0000000013171000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BlackGuard, Description: Yara detected BlackGuard, Source: 00000000.00000002.410785101.0000000013171000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.410785101.0000000013171000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC0B8CF1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC0B8CF1E9	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0B79B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0B79B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0B8712E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0B7A2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFC0B8712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0B8712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFC0B8712E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0B79B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC0B79B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC0B8712E7	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FFC0B8955FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FFC0B8955FA	unknown
C:\Users\user\Desktop\file.exe	unknown	4096	success or wait	1	7FFC0B8955FA	unknown
C:\Users\user\Desktop\file.exe	unknown	512	success or wait	1	7FFC0B8955FA	unknown

Analysis Process: WerFault.exe PID: **5956**, Parent PID: **3360**

General

Target ID:	3
Start time:	17:22:17
Start date:	06/06/2023
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 3360 -s 944
Imagebase:	0x7ff679980000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	7FFC0F13527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E4D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E4D.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_d2892c472895a2b98efdcdcd7642ab4d7ea6c2_3b20dbdc_17059a9d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_d2892c472895a2b98efdcdcd7642ab4d7ea6c2_3b20dbdc_17059a9d\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC0F12E9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E4D.tmp	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E4D.tmp.xml	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6B.tmp.csv	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F37.tmp.txt	success or wait	1	7FFC0F12E9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd fd 7f 64 fd 05 12 00 00 00 00 00	MDMP d	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	8744	6	00 00 00 00 00 00		success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	212	1420	09 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 28 22 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 60 fd 09 02 00 00 54 05 00 00 fd 03 00 00 20 0d 00 00 fd fd 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UB("Lw`T d0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	10252	1232	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 65 0a fd 7f 00 00 fd 00 2a 01 00 00 00 00 01 00 00 00 00 00 00 00 fd 65 70 0b fd 7f 00 00 4f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 06 02 00 00 60 1b 17 03 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 00 00 00 00 00 30 fd fd 00 00 00 00 00 0c fd 70 0b fd 7f 00 00 58 fd fd 00 00 00 00 00 01 00 00 00 00 00 00 00 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 fd fd 00 00 00 00 00 05 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 61 3c 37 47 fd 0b 00 00 29 23 fd 0b fd 7f 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 52 43 43 fd 00 00 00 00 18 19 17 03 00 00 00 00 18 fd 2e fd 7f 00	e*epO3++S++`0pXha<7 G)#@RCC.	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	1632	168	38 09 00 00 00 00 00 00 52 43 43 fd 01 00 00 00 00 00 00 00 00 00 00 00 18 fd 2e fd 7f 00 00 05 00 00 00 00 00 00 00 0e 00 02 fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 0b fd 7f 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 01 00 00 00 00 00 00 00 60 03 72 00 00 00 00 00 d1 fd 47 fd 0b 00 00 68 fd fd 0b fd 7f 00 00 fd 00 2a 01 00 00 00 00 49 56 fd 0b fd 7f 00 00 00 00 00 00 00 00 00 fd 04 00 00 0c 28 00 00	8RCC.p`rGh*IV(	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	18876	20	fd 01 00 00 40 4e fd 0a fd 7f 00 00 fd 02 00 00 00 68 00 00	@Nh	success or wait	484	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	26624	712	00 00 00 01 70 00 00 00 66 01 fd 05 57 00 06 00 fd 29 fd 0a fd 7f 00 00 00 10 17 0a fd 7f 00 00 48 6a 17 0a fd 7f 00 00 78 35 24 0a fd 7f 00 00 fd 02 00 00 00 00 00 00 fd 4e fd 0a fd 7f 00 00 10 4f fd 0a fd 7f 00 00 50 4f fd 0a fd 7f 00 00 fd 4f fd 0a fd 7f 00 00 fd 4f fd 0a fd 7f 00 00 10 50 fd 0a fd 7f 00 00 68 fd 7f 0a fd 7f 00 00 50 50 fd 0a fd 7f 00 00 fd fd 7f 0a fd 7f 00 00 fd fd 7f 0a fd 7f 00 00 fd 50 fd 0a fd 7f 00 00 fd 50 fd 0a fd 7f 00 00 30 00 00 00 00 00 00 00 08 fd 0a fd 7f 00 00 70 fd 0a fd 7f 00 00 40 fd 0a fd 7f 00 00 fd fd fd 0a fd 7f 00 00 fd fd fd 0a fd 7f 00 00 fd 08 fd 0a fd 7f 00 00 00 fd 5a 0a fd 7f 00 00 fd fd 68 0a fd 7f 00 00 40 fd 63 0a fd 7f 00 00 fd fd 64 0a fd 7f 00 00 20 6e 67 0a fd 7f 00 00 fd 71 62 0a fd 7f 00	pfW)Hjx5$NOPOOOPhPPPP0p@Zh@cd ngqb	success or wait	483	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	274728	8	d1 fd 47 fd 0b 00 00	G	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	1800	4	06 00 00 00		success or wait	6	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	11484	1232	20 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 20 03 00 00 00 00 00 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd 48 fd fd 00 00 00 00 00 fd fd fd fd fd fd fd 48 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 48 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 0e 32 fd 7f 00	3++S++FHHH2	success or wait	6	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	2044	48	08 1b 00 00 01 00 00 00 20 00 00 00 02 00 00 00 00 fd 05 01 00 00 00 00 78 fd 6d 1b 00 00 00 00 fd 0a 00 00 3e fd 02 00 fd 04 00 00 fd 44 00 00	xm>D	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	2104	4	31 00 00 00	1	success or wait	49	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	8750	22	10 00 00 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 00 00	file.exe	success or wait	49	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	7292	792	00 00 73 07 fd 7f 00 00 00 fd 13 00 3d fd 13 00 fd 5f fd 5a fd 27 00 00 fd 04 fd fd 00 00 01 00 07 00 0e 00 00 00 fd 0b 07 00 0e 00 00 00 fd 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 02 00 00 00 00 00 00 00 00 00 00 fd fd fd 7f 00 00 00 00 fd fd fd 7f 00 00 00 00 fd fd fd 7f 00 00 18 00 00 00 00 00 00 00 fd 4b 2f 01 00 00 00 00 fd fd 1b 32 fd 7f 00 00 fd 2c 01 00 00 00 00 fd 10 1e 17 98 fd 01 00 00 fd fd fd 7f 00 00 00 00 fd fd fd 7f 00 00 00 00 fd fd fd 7f 00 00 fd 55 fd 0b fd 7f 00 00 fd 2c 01 00 00 00 00 20 16 2f 01 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00	s=_Z'?)`A pK/2,U, /	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	8100	644	01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 30 fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 6b fd 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 45 fd 03 00 00 00 00 fd 28 04 00 00 00 00 00 00 00 00 00 00 00 00 1c fd 1a 00 00 00 00 00 24 66 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6b 05 00 00 00 00 00 48 12 fd fd 00 00 00 00 04 fd 75 1f 00 00 00 00 7f fd fd 17 00 00 00 00 fd fd fd 01 00 00 00 00 2c fd 00 00 3c 2b 01 00 fd fd 06 00 60 6c 0a 00 24 66 05 00 06 fd 1f 00 fd 6b 05 00 fd fd 25 00 40 45 01 00 fd fd 12 00 00 00 00 00 fd 40 13 00 fd fd 04 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00	Zb0kE($f@kHu, <+`l$fk%@E@	success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	274736	15232	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7C19.tmp.dmp	32	120	03 00 00 00 24 01 00 00 08 07 00 00 04 00 00 00 fd 14 00 00 38 08 00 00 0d 00 00 00 fd 02 00 00 fd 1c 00 00 05 00 00 00 44 1e 00 00 fd 49 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 40 25 00 00 70 47 04 00 15 00 00 00 fd 01 00 00 fd 1f 00 00 16 00 00 00 fd 00 00 00 fd 21 00 00	$8DI`8T@%pG!	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.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	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3360</Pid>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 69 00 6c 00 65 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>file.exe</ImageName>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1072	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1170	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 35 00 31 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>12513</Uptime>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1222	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1300	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1304	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1308	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	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1360	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1364	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1368	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1412	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1416	2	09 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1422	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 39 00 32 00 30 00 33 00 35 00 36 00 38 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4920356864</PeakVirtualSize>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1512	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1516	2	09 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1522	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 39 00 32 00 30 00 33 00 34 00 38 00 36 00 37 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>4920348672</VirtualSize>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1596	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1600	2	09 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1606	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 31 00 31 00 33 00 36 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>11363</PageFaultCount>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1682	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1686	2	09 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1692	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 34 00 35 00 32 00 30 00 37 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>45207552</PeakWorkingSetSize>	success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1800	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 34 00 35 00 32 00 30 00 37 00 35 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>45207552</WorkingSetSize>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 30 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>340352</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2016	98	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 33 00 34 00 30 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>340352</QuotaPagedPoolUsage>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2124	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 30 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>190504</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2250	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2254	2	09 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2260	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 30 00 32 00 33 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>190232</QuotaNonPagedPoolUsage>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2370	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2374	2	09 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2380	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 31 00 37 00 39 00 39 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>36179968</PagefileUsage>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2458	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2462	2	09 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2468	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 31 00 38 00 38 00 31 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>36188160</PeakPagefileUsage>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2562	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2566	2	09 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2572	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 31 00 37 00 39 00 39 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>36179968</PrivateUsage>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2646	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2650	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2654	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2700	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2704	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2708	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2738	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2742	2	09 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2748	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2788	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2792	2	09 00		success or wait	4	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2800	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2830	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2834	2	09 00		success or wait	4	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2842	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2912	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2916	2	09 00		success or wait	4	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	2924	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000</CmdLineSignature>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3014	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3018	2	09 00		success or wait	4	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3026	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 39 00 37 00 32 00 39 00 36 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>3972962</Uptime>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3086	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3176	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3240	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3298	96	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 32 00 32 00 30 00 33 00 39 00 38 00 31 00 31 00 33 00 39 00 39 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2203981139968</PeakVirtualSize>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3394	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3398	2	09 00		success or wait	5	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3408	80	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 32 00 32 00 30 00 33 00 39 00 35 00 34 00 33 00 37 00 36 00 37 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203954376704</VirtualSize>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3488	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3492	2	09 00		success or wait	5	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3502	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 38 00 36 00 37 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>68679</PageFaultCount>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3578	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3582	2	09 00		success or wait	5	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3592	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 35 00 30 00 37 00 39 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>125079552</PeakWorkingSetSize>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3692	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3696	2	09 00		success or wait	5	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3706	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 39 00 34 00 32 00 37 00 30 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>119427072</WorkingSetSize>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3790	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3794	2	09 00		success or wait	5	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3804	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 39 00 39 00 37 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>119976</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3920	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3924	2	09 00		success or wait	5	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	3934	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 31 00 35 00 34 00 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1154416</QuotaPagedPoolUsage>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4034	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4038	2	09 00		success or wait	5	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4048	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 39 00 32 00 35 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>92528</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4172	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4176	2	09 00		success or wait	5	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4186	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 34 00 30 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>84016</QuotaNonPagedPoolUsage>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4294	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4298	2	09 00		success or wait	5	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4308	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 32 00 30 00 37 00 38 00 32 00 30 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>42078208</PagefileUsage>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4386	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4390	2	09 00		success or wait	5	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4400	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 39 00 34 00 35 00 39 00 32 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>49459200</PeakPagefileUsage>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4494	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4498	2	09 00		success or wait	5	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4508	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 32 00 30 00 37 00 38 00 32 00 30 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>42078208</PrivateUsage>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4582	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4586	2	09 00		success or wait	4	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4594	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4640	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4644	2	09 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4650	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4692	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4696	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4700	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4732	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4736	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4738	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4780	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4784	2	09 00		success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4786	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4832	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 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>CLR20r3</EventType>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4892	4	0d 00 0a 00		success or wait	9	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4896	2	09 00		success or wait	18	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	4900	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 66 00 69 00 6c 00 65 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>file.exe</Parameter0>	success or wait	9	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	5602	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	5606	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	5608	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	5648	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	5652	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	5654	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	5692	4	0d 00 0a 00		success or wait	6	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	5696	2	09 00		success or wait	12	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	5700	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6254	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6258	2	09 00		success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6260	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6300	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6304	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6306	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6344	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6348	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6352	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6446	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6450	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6454	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 73 00 65 00 6d 00 63 00 74 00 62 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>semctb, Inc.</SystemManufacturer>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6560	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6564	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6568	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 73 00 65 00 6d 00 63 00 74 00 62 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>semctb7,1</SystemProductName>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6664	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6668	2	09 00		success or wait	2	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6672	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6792	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6796	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6800	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 34 00 35 00 32 00 34 00 38 00 39 00 35 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1645248950</OSInstallDate>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6882	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6886	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6890	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6992	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	6996	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7000	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7068	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7072	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7074	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7114	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7118	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7120	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7154	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7158	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7162	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7258	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7262	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7264	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7300	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7304	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7306	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7330	4	0d 00 0a 00		success or wait	3	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7334	2	09 00		success or wait	6	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7338	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7596	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7600	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7602	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7628	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7632	2	09 00		success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7634	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 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 30 00 3a 00 32 00 32 00 3a 00 31 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T00:22:18Z">	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7734	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7738	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	7742	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 33 00 37 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 33 00 36 00 30 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 31 00 34 00 33 00 37 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 31 00 34 00 33 00 37 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="370" PID="3360" UptimeMS="11437" TimeSinceCreationMS="11437" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8008	4	0d 00 0a 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8012	2	09 00		success or wait	6	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8018	184	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 34 00 31 00 30 00 38 00 32 00 38 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="4108288" TimelineUnitShift="12" Timeline="1111"/>	success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8398	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8402	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8406	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8426	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8430	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8432	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8470	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8474	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8476	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8514	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8518	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8522	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 35 00 64 00 36 00 61 00 30 00 33 00 64 00 2d 00 31 00 32 00 32 00 63 00 2d 00 34 00 38 00 38 00 33 00 2d 00 39 00 39 00 38 00 38 00 2d 00 65 00 61 00 37 00 36 00 33 00 36 00 63 00 65 00 62 00 33 00 37 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>e5d6a03d-122c-4883-9988-ea7636ceb37a</Guid>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8620	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8624	2	09 00		success or wait	2	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8628	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 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 30 00 3a 00 32 00 32 00 3a 00 31 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-07T00:22:18Z</CreationTime>	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8726	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8730	2	09 00		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8732	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8772	4	0d 00 0a 00		success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E1E.tmp.WERInternalMetadata.xml	8776	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	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E4D.tmp.xml	0	4781	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_d2892c472895a2b98efdcdcd7642ab4d7ea6c2_3b20dbdc_17059a9d\Report.wer	0	2	fd fd		success or wait	1	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_d2892c472895a2b98efdcdcd7642ab4d7ea6c2_3b20dbdc_17059a9d\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	176	7FFC0F12E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_d2892c472895a2b98efdcdcd7642ab4d7ea6c2_3b20dbdc_17059a9d\Report.wer	12934	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 36 00 37 00 36 00 36 00 35 00 35 00 34 00 31 00 35 00	MetadataHash=-1676655415	success or wait	1	7FFC0F12E9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC0F12E3FE	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	ProgramId	unicode	0006b33f2f13c16538302ca681bf7140694000000000	success or wait	1	7FFC0F151D2D	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	FileId	unicode	0000056a3fbe0a88a39348e8b99f0cffb3c6e63b5655	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	LowerCaseLongPath	unicode	c:\users\user\desktop\file.exe	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	LongPathHash	unicode	file.exe|4de4a562939a1599	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	Name	unicode	file.exe	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	Publisher	unicode	python software foundation	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	Version	unicode	3.11.3150.1013	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	BinFileVersion	unicode	3.11.3150.1013	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	BinaryType	unicode	pe32_clr_il	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	ProductName	unicode		success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	ProductVersion	unicode	3.11.3150.1013	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	LinkDate	unicode	05/23/2023 12:48:17	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	BinProductVersion	unicode	3.11.3150.1013	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	Size	B	00 DE 37 00 00 00 00 00	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	Language	dword	0	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	IsPeFile	dword	1	success or wait	1	7FFC0F151D2D	unknown
\REGISTRY\A\{a10d5d40-de29-ad1b-d8c4-b12ef076432c}\Root\InventoryApplicationFile\file.exe|4de4a562939a1599	IsOsComponent	dword	0	success or wait	1	7FFC0F151D2D	unknown

Key Value Modified								
Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 D0 3E AF DE FC 7F 00 00 01 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	52 43 43 E0 01 00 00 00 00 00 00 00 00 00 00 00 18 F2 A0 2E FC 7F 00 00 05 00 00 00 00 00 00 00 0E 00 02 80 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 0B FC 7F 00 00 00 00 00 00 00 00 00 00 00 FE FF FF FF FF FF FF FF E8 E9 FA 00 00 00 00 00 01 00 00 00 00 00 00 00 60 03 72 00 00 00 00 00 CF 91 8C 47 D5 0B 00 00 68 B1 E1 0B FC 7F 00 00 F0 00 2A 01 00 00 00 00 49 56 83 0B FC 7F 00 00 00 00 00 00 00 00 00	success or wait	1	7FFC0F1507CB	RegSetValueExW

Disassembly

No disassembly