ID: 691234
Sample Name:
OatAFVzm15.exe
Cookbook: default.jbs
Time: 03:58:55
Date: 27/08/2022
Version: 35.0.0 Citrine

Table of Contents

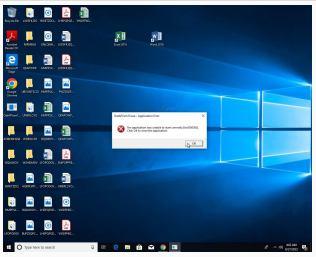
Windows Analysis Report

OatAFVzm15.exe

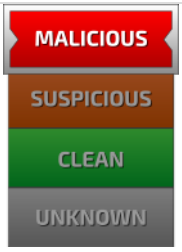
Overview

General Information

Sample Name:	OatAFVzm15.exe
Analysis ID:	691234
MD5:	b741daeca2edb8..
SHA1:	4affabf1f09e55a…
SHA256:	c688c3da0b3fe2…
Tags:	exe zeus2
Infos:	



Detection



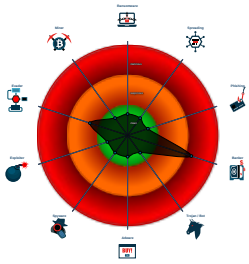
Citadel

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Yara detected Citadel
- Multi AV Scanner detection for subm…
- Machine Learning detection for sam…
- Uses 32bit PE files
- Yara signature match
- Antivirus or Machine Learning detec…
- One or more processes crash
- PE file contains an invalid checksum
- Checks if the current process is bei…
- Entry point lies outside standard sec…

Classification



Process Tree

- **System is w10x64**
- OatAFVzm15.exe (PID: 772 cmdline: "C:\Users\user\Desktop\OatAFVzm15.exe" MD5: B741DAECA2EDB8D539BE2938E5F9490F)
  - WerFault.exe (PID: 6092 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 772 -s 212 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
OatAFVzm15.exe	JoeSecurity_Citadel	Yara detected Citadel	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.249623287.0000000000401000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Citadel	Yara detected Citadel	Joe Security	
00000001.00000000.248127496.0000000000401000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Citadel	Yara detected Citadel	Joe Security	
00000001.00000002.644531481.0000000000401000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Citadel	Yara detected Citadel	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000000.250108543.0000000000401000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Citadel	Yara detected Citadel	Joe Security	
Process Memory Space: OatAFVzm15.exe PID: 772	JoeSecurity_Citadel	Yara detected Citadel	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.OatAFVzm15.exe.400000.0.unpack	JoeSecurity_Citadel	Yara detected Citadel	Joe Security	
1.0.OatAFVzm15.exe.400000.2.unpack	JoeSecurity_Citadel	Yara detected Citadel	Joe Security	
1.0.OatAFVzm15.exe.400000.1.unpack	JoeSecurity_Citadel	Yara detected Citadel	Joe Security	
1.2.OatAFVzm15.exe.400000.0.unpack	JoeSecurity_Citadel	Yara detected Citadel	Joe Security	

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

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Citadel

E-Banking Fraud

Yara detected Citadel

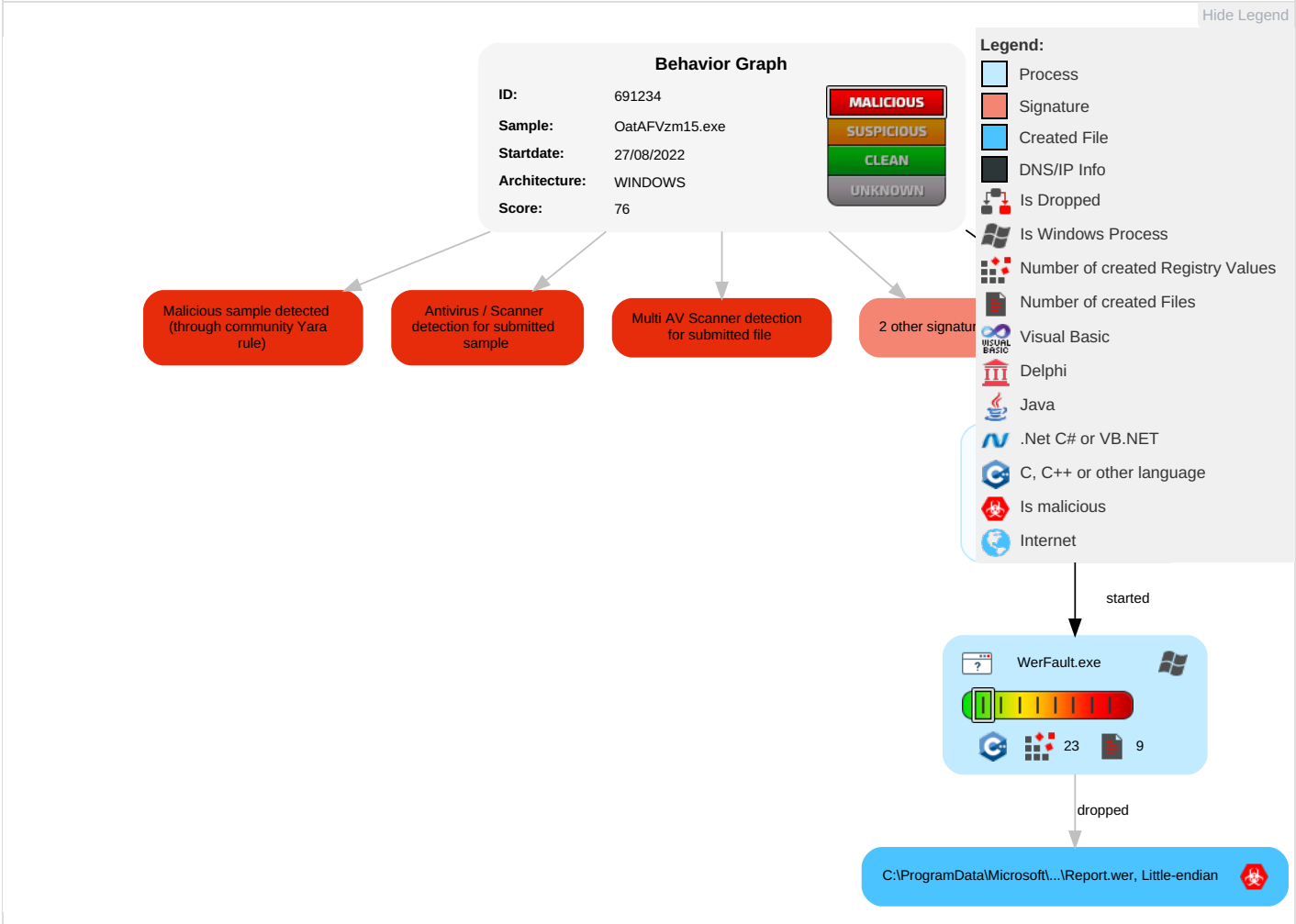
System Summary

Malicious sample detected (through community Yara rule)

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	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 Software Packing	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 Process Injection	Security Account Manager	1 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)	Binary Padding	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

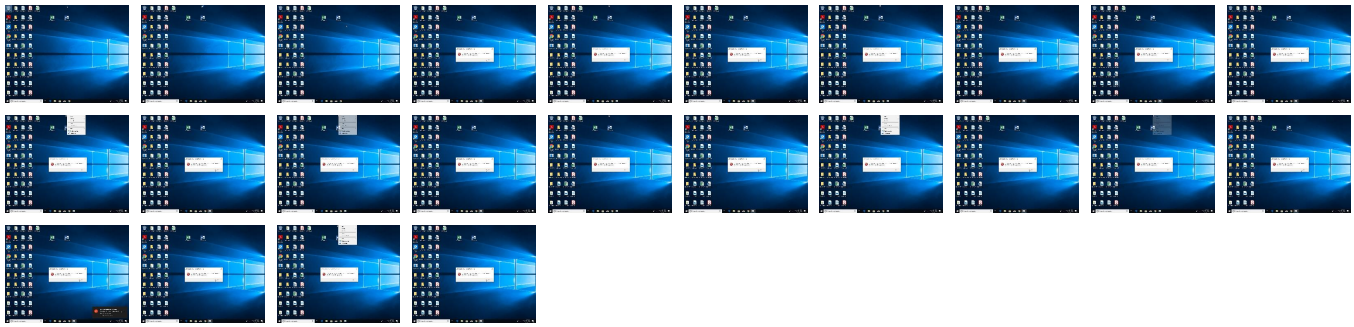
Behavior Graph



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
OatAFVzm15.exe	57%	Metadefender		Browse
OatAFVzm15.exe	92%	ReversingLabs	Win32.Trojan.Zeus	
OatAFVzm15.exe	100%	Avira	TR/Spy.Gen	
OatAFVzm15.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.OatAFVzm15.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File
1.0.OatAFVzm15.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen		Download File
1.0.OatAFVzm15.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File
1.0.OatAFVzm15.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen		Download File

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://www.google.com/webhp	OatAFVzm15.exe	false		high
http://www.google.com/webhpbcU	OatAFVzm15.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	691234
Start date and time:	2022-08-27 03:58:55 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OatAFVzm15.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal76.bank.winEXE@2/4@0/0
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 • Adjust boot time • Enable AMSI • Sleeps bigger than 300000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.42.73.29
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, login.live.com, eudb.ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: OatAFVzm15.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_OatAFVzm15.exe_a263187443166683b0d1fe53934c2b47109f797_532d33bc_179a95d5\Report.wer

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

Size (bytes):	65536
Entropy (8bit):	0.8477355130975469
Encrypted:	false
SSDEEP:	96:0FOFfc6hFNhM1Dg3f6UpXIQcQzc6CmcE1cw3CH+HbHg/opAnQ0DF16Fawn9TxifT:049Lh8iHNXfnjJ/u7suS274It0i
MD5:	67ED49590B71E87BC8AEF7FED35BEDA5
SHA1:	17943598405BF7ADEE1A6D940C728B98C7CFFEF5
SHA-256:	FFE956B2D85E2C8FABFB8AC382C63DB6D2F283BF7366439F1CE9D7FDD58AB76D
SHA-512:	F8A9380C2DFFDB7691CE32EDDE652318D89DD76BA2B1D760B512B0B1F4B628C8CEAF71CC9962F975CE13A6EA13F7C5B46557FC4D4BC8CC61114E1FFF3ECB/0AF
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.6.0.7.1.5.9.0.8.8.1.3.7.0.5.....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.=.1.3.3.0.6.0.7.1.5.9.2.4.2.8.2.3.2.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.4.a.e.f.a.5.d.-.3.0.d.9.-.4.5.3.0.-.8.4.9.6.-.e.9.3.6.f.3.3.f.2.5.b.9.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.8.2.8.c.0.d.5.-.a.2.b.a.-.4.5.7.f.-.8.b.d.3.-.9.7.2.2.d.7.f.a.d.b.5.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.O.a.t.A.F.V.z.m.1.5...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.3.0.4.-.0.0.0.1.-.0.0.1.f.-.2.3.5.9.-.a.9.1.f.0.4.b.a.d.8.0.1...T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.5.7.6.f.6.0.9.7.1.0.f.3.c.d.f.0.6.3.5.7.7.d.c.7.a.5.8.c.7.e.c.e.0.0.0.0.f.f.f.f.!.0.0.0.0.4.a.f.f.a.b.f.1.f.0.9.e.5.5.a.1.7.7.7.f.e.d.b.e.8.3.f.c.2.6.9.0.5.9.4.3.0.4.5.c.!.O.a.t.A.F.V.z.m.1.5...e.x.e.....T.a.r.g.e.t.A.p.p.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Aug 27 10:59:51 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	34716
Entropy (8bit):	2.202131923820371
Encrypted:	false
SSDEEP:	192:ZkBBj9VBsiv0O65OsdSN591U03PjKHyl6DBQCW:aJVBsQ6rY5jKxBXW
MD5:	45472289EA981225005104219636EC68
SHA1:	28675A39F6405261955670E64A2092D0699D6B9D
SHA-256:	038786401FD022238B42FA9231B7CF4682E150676FF567A892B3CCACF5DA4962
SHA-512:	387D498F6D8B904849EFF2F28384BA4312A69C975EE5DC45C562F7525BC0C6C7046802541174239E7E5B9E90C0DFE935FD9537C8F2BEE511B00F16463C4B680E
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....'..c.....4.....(.....T.....8.....T.....U.....B.....T.....GenuineIntelW.....T.....$..c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8284
Entropy (8bit):	3.6967453155481205
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNija6F6YqbSUMLrgmf2QjS3OzCpxT89bESsfiGsm:RrlsNie6F6YWSUMngmf2QjS3O9ERfd
MD5:	66631305A7D025E8E6DE30003254E753
SHA1:	9BA48BE6C3EA2D67A691F793850901C59A5ACE21
SHA-256:	FEA2674FE4A504EFE873738BA4433B61BE9211955148464134B824873AC01B2F
SHA-512:	09864257CB92A302C4132094C61BDC5E61AEAAE7ECA427376421A8E795CA8DAA3967F25DB06F28D8026325291DA6BA97A52FE9A122004573821D330035825504
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.>.7.7.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	4567
Entropy (8bit):	4.4595943412768975
Encrypted:	false
SSDEEP:	48:cvlwSD8zsdJgtWI90SWgc8sqYjf8fm8M4JPlF/c+q8vA2pjusNVMlOd:uITf3PzgrsqYYJsPgju2VMlOd
MD5:	2E9D1069FB8B86985BBC56341C8458B5
SHA1:	46C27DD82AA8C2F31EC1BBB149B8D576EA54CA6C
SHA-256:	1B4B6082E07DF792F627F9E3E1025B99278F6AB0842669BC1D4CB390FA1ACB96
SHA-512:	2F40A7A399B517D5C9F94BCFB600AED642E1D7346F67AF65D44E47B0800FCA9D21B288D46B8069C499D7B20CF1599B0A1DDD9E05415699EAA65FECB5FA06A911
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="1665850" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	3.4408516130120472
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Clipper DOS Executable (2020/12) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Lumena CEL bitmap (63/63) 0.00%
File name:	OatAFVzm15.exe
File size:	267264
MD5:	b741daeca2edb8d539be2938e5f9490f
SHA1:	4affabf1f09e55a1777fedbe83fc26905943045c
SHA256:	c688c3da0b3fe263e2441f884d47966bb74875c94564e7694aa1c462e5c9435f
SHA512:	f43fac8e1ab37c70c6633cd558fd9d164fea51cd1835086cdaf42aff60d2b444626b609d4af5f627953913bcf6fc4a0dd1bb39737dc0e23b1bd3bd61930edd20
SSDEEP:	3072:E/DD2zNc31I3tgt89I51ceYaQHK3HEEooVj9k:E/hCdgtR569aQuHEcVj9
TLSH:	6844BF5BB98184B7D5BA3B709DA8B23663FF8D24242DCD87E7580D993831861F22D307
File Content Preview:	MZ.....@.....PE..L..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x403ee5
Entrypoint Section:	.data
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x408FF235 [Wed Apr 28 18:04:37 2004 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	7
OS Version Minor:	2
File Version Major:	7

File Version Minor:	2
Subsystem Version Major:	7
Subsystem Version Minor:	2
Import Hash:	f3b6157e0baac9b50d25d58c877c29ad

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
sub esp, 6Ch
push esi
push dword ptr [ebp+0Ch]
lea eax, dword ptr [ebp-68h]
push eax
push dword ptr [ebp+08h]
call 00007F36E0770AC7h
lea eax, dword ptr [ebp-68h]
push eax
push 00000000h
push 0041A2CCh
call dword ptr [004011A4h]
test eax, eax
je 00007F36E0770B1Bh
mov esi, eax
call 00007F36E0777CB3h
jmp 00007F36E0770B14h
xor eax, eax
pop esi
leave
retn 0008h
push ebp
mov ebp, esp
push ecx
push ecx
mov eax, dword ptr [0041A2A4h]
push ebx
push edi
call 00007F36E0779029h
xor ebx, ebx
mov dword ptr [ebp-08h], eax
cmp eax, ebx
jne 00007F36E0770B19h
xor eax, eax
jmp 00007F36E0770BD3h
push 00000002h
push ebx
push ebx
lea eax, dword ptr [ebp+08h]
push eax
push edi
push dword ptr [ebp+08h]
mov byte ptr [ebp-01h], bl
push FFFFFFFFh
call dword ptr [004011F4h]
test eax, eax
jne 00007F36E0770B16h
mov byte ptr [ebp-01h], 00000001h
push esi
mov esi, dword ptr [004011E0h]
push ebx

Instruction
push 00000004h
lea ecx, dword ptr [ebp+0Ch]
push ecx
mov ecx, dword ptr [ebp-08h]
mov eax, 0041A290h
sub eax, dword ptr [0041A2A4h]
add eax, ecx
push eax
push edi
call esi
test eax, eax
jne 00007F36E0770B15h
inc byte ptr [ebp-01h]
push ebx
push 00000004h
lea ecx, dword ptr [ebp-08h]
push ecx
mov ecx, dword ptr [ebp-08h]
mov eax, 0041A2A4h
sub eax, dword ptr [0041A2A4h]
add eax, ecx
push eax
push edi
call esi
pop esi
test eax, eax
jne 00007F36E0770B15h
inc byte ptr [ebp-01h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1200	0xd20178	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x40000	0xf0	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x21000	0x4d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x1000	0x4000	0x4000	False	0.5638427734375	data	5.9940228845162915	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x5000	0x1000	0x1000	False	0.588623046875	data	6.193572249131582	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x6000	0x1b000	0x1b000	False	0.49233217592592593	data	5.64920698370386	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x21000	0x1f000	0x1f000	False	0.0011498235887096775	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.idata	0x40000	0x1400	0x1400	False	0.4671875	data	5.092882560692016	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Imports

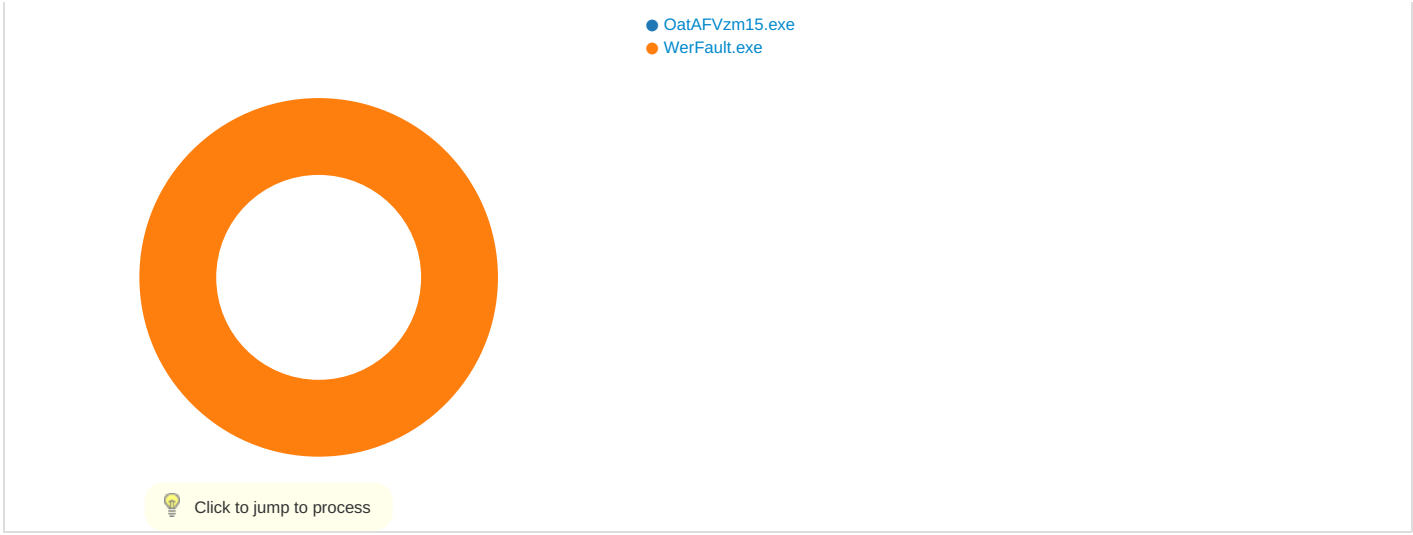
DLL	Import
ADVAPI32.dll	RegCloseKey, CryptCreateHash, LookupPrivilegeValueW, SetNamedSecurityInfoW, SetSecurityDescriptorDacl, InitializeSecurityDescriptor, CreateProcessAsUserW, RegQueryValueExW, CryptReleaseContext, RegCreateKeyExW, GetTokenInformation, GetSidSubAuthorityCount, OpenThreadToken, CryptAcquireContextW, GetSidSubAuthority, OpenProcessToken, CryptGetHashParam, RegEnumKeyExW, RegOpenKeyExW, GetLengthSid, IsWellKnownSid, GetSecurityDescriptorSacl, SetSecurityDescriptorSacl, CryptDestroyHash, AdjustTokenPrivileges, ConvertSidToStringSidW, RegSetValueExW, CryptHashData, EqualSid, InitiateSystemShutdownExW, ConvertStringSecurityDescriptorToSecurityDescriptorW
CRYPT32.dll	CertDeleteCRLFromStore, CertCloseStore, PFXImportCertStore, CertEnumCertificatesInStore, CertDuplicateCRLContext, PFXExportCertStoreEx, CertOpenSystemStoreW
KERNEL32.dll	CreateProcessW, HeapAlloc, SystemTimeToFileTime, SetFilePointerEx, HeapFree, CreateDirectoryW, GetComputerNameW, GetTickCount, GetCurrentThread, GetProcessHeap, IsBadReadPtr, SetFileTime, VirtualQueryEx, WriteFile, OpenProcess, Thread32First, WideCharToMultiByte, ReadProcessMemory, GetVersionExW, HeapDestroy, HeapCreate, GetFileAttributesW, Thread32Next, ReadFile, GetTimeZoneInformation, CreateFileW, MultiByteToWideChar, FlushFileBuffers, GetTempPathW, GetFileSizeEx, FreeLibrary, GetEnvironmentVariableW, SetLastError, VirtualProtectEx, VirtualAllocEx, FindClose, LoadLibraryA, RemoveDirectoryW, FindNextFileW, VirtualProtect, CreateToolhelp32Snapshot, GetFileTime, ReleaseMutex, FileTimeToLocalFileTime, GetVolumeNameForVolumeMountPointW, DeleteFileW, GetFileInformationByHandle, GetSystemTime, SetFileAttributesW, CreateThread, CreateRemoteThread, Process32FirstW, Process32NextW, lstrcmpi, WTSGetActiveConsoleSessionId, SetThreadPriority, GetLocalTime, GlobalLock, GlobalUnlock, ResetEvent, MoveFileExW, GetUserDefaultUILanguage, SetEndOfFile, GetNativeSystemInfo, FindFirstFileW, CreateMutexW, HeapReAlloc, GetTempFileNameW, OpenMutexW, FileTimeToDosDateTime, GetProcessId, EnterCriticalSection, VirtualAlloc, LeaveCriticalSection, InitializeCriticalSection, SetThreadContext, GetThreadContext, ExpandEnvironmentStringsW, GetPrivateProfileIntW, GetPrivateProfileStringW, WriteProcessMemory, LocalFree, GetCurrentProcessId, CloseHandle, ExitProcess, DuplicateHandle, OpenEventW, GetFileAttributesExW, lstrcmpiW, WaitForMultipleObjects, CreateEventW, GetProcAddress, GetModuleFileNameW, Sleep, VirtualFreeEx, VirtualFree, GetModuleHandleW, SetEvent, WaitForSingleObject, SetErrorMode, GetCommandLineW, GetLastError
NETAPI32.dll	NetUserEnum, NetApiBufferFree, NetUserGetInfo
OLEAUT32.dll	VariantInit, VariantClear, SysAllocString, SysFreeString
SHELL32.dll	CommandLineToArgvW, SHGetFolderPathW, ShellExecuteW
SHLWAPI.dll	wvnsprintfW, PathIsDirectoryW, PathFindFileNameW, PathAddBackslashW, SHDeleteValueW, PathSkipRootW, SHDeleteKeyW, PathRemoveBackslashW, UrlUnescapeA, PathRenameExtensionW, PathMatchSpecW, StrCmpNIA, wvnsprintfA, PathUnquoteSpacesW, PathQuoteSpacesW, PathIsURLW, StrStrIW, PathRemoveFileSpecW, PathAddExtensionW, StrStrIA, PathCombineW, StrCmpNIW
Secur32.dll	GetUserNameExW
USER32.dll	DrawIcon, LoadImageW, CharLowerBuffA, CharLowerW, ToUnicode, GetClipboardData, GetKeyboardState, ExitWindowsEx, GetIconInfo, DispatchMessageW, CharUpperW, PeekMessageW, CharLowerA, TranslateMessage, CharToOemW, MsgWaitForMultipleObjects, GetCursorPos
WININET.dll	InternetCrackUrlA, HttpAddRequestHeadersW, InternetSetStatusCallbackW, GetUrlCacheEntryInfoW, HttpSendRequestW, InternetReadFileExA, InternetQueryDataAvailable, HttpSendRequestExW, HttpSendRequestExA, HttpAddRequestHeadersA, InternetQueryOptionA, InternetCloseHandle, InternetOpenA, HttpSendRequestA, HttpOpenRequestA, InternetSetOptionA, InternetReadFile, InternetConnectA, HttpQueryInfoA
WS2_32.dll	WSASetLastError, closesocket, FreeAddrInfoW, listen, socket, recv, sendto, WSASend, WSAEventSelect, getpeername, WSAIoctl, connect, WSAAddressToStringW, WSAStartup, recvfrom, getaddrinfo, select, WSAGetLastError, getsockname, shutdown, setsockopt, send, accept, bind
ole32.dll	StringFromGUID2, CLSIDFromString, CoUninitialize, CoCreateInstance, CoInitializeEx

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: OatAFVzm15.exe PID: 772, Parent PID: 5412

General	
Target ID:	1
Start time:	03:59:48
Start date:	27/08/2022
Path:	C:\Users\user\Desktop\OatAFVzm15.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\OatAFVzm15.exe"
Imagebase:	0x400000
File size:	267264 bytes
MD5 hash:	B741DAECA2EDB8D539BE2938E5F9490F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Citadel, Description: Yara detected Citadel, Source: 00000001.00000000.249623287.0000000000401000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Citadel, Description: Yara detected Citadel, Source: 00000001.00000000.248127496.0000000000401000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Citadel, Description: Yara detected Citadel, Source: 00000001.00000002.644531481.0000000000401000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Citadel, Description: Yara detected Citadel, Source: 00000001.00000000.250108543.0000000000401000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: WerFault.exe PID: 6092, Parent PID: 772

General	
Target ID:	3
Start time:	03:59:50
Start date:	27/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 772 -s 212
Imagebase:	0xcb0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D4D1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_OatAFVzm15.exe_a26318744316683b0d1fe53934c2b47109f797_532d33bc_179a95d5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_OatAFVzm15.exe_a26318744316683b0d1fe53934c2b47109f797_532d33bc_179a95d5\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4C497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.xml	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD147.tmp.csv	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD167.tmp.txt	success or wait	1	6D4C497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 27 fd 09 63 fd 05 12 00 00 00 00 00	MDMP 'c	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	6484	6	00 00 00 00 00 00		success or wait	1	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 54 19 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 04 03 00 00 24 fd 09 63 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 00 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	UBTGenuineIntelWT$c0 Pacific Standard TimePacific Daylight Time	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	7556	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 fd 76 14 01 44 00 fd fd 19 00 00 10 40 00 40 fd 76 fd fd 76 fd fd 19 00 fd fd 77 23 00 00 00 46 02 01 00 38 fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++vD@@vvw#F8+	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	1620	168	30 0f 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 77 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 10 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 1d 00 00	0w@	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	10420	20	11 00 00 00 00 50 21 00 00 00 00 00 fd 04 00 00 fd 29 00 00	P!)	success or wait	17	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	10696	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 28 17 5e 00 00 00 00 00 00 00 5e 00 fd 79 fd 77 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 01 00 01 00 00 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 01 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@{w(^^yw{w0(Pm `fwPSwB	success or wait	16	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	30680	572	fd fd fd 77 fd 4c 77 fd 00 00 00 fd fd fd fd 10 00 00 00 58 fd fd 00 24 fd fd 00 fd fd fd fd 40 cc 77 40 cc 77 10 5c 5e 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 00 00 fd fd fd fd 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 3e 5f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 21 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 5c 5e 00 00 00 00 00 fd fd fd fd fd fd fd 54 52 21 00 fd fd 7d 00 48 5c 5e 00 fd fd 7d 00 00 00 00 00 fd fd fd fd 10 5c 5e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwX$@w@w\^H>_P!\^TR!}H\^}\^	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	8272	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 10 40 00 40 fd 76 00 00 00 00 24 fd 19 00 fd fd fd 77 23 00 00 00 06 02 00 00 fd fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++@@v$w#+	success or wait	3	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	1888	48	fd 17 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 21 00 00 00 00 00 fd fd fd 00 00 00 00 00 3c 02 00 00 fd 77 00 00 fd 02 00 00 fd 25 00 00	!<w%	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	1948	4	24 00 00 00	$	success or wait	36	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	6490	34	1c 00 00 00 4f 00 61 00 74 00 41 00 46 00 56 00 7a 00 6d 00 31 00 35 00 2e 00 65 00 78 00 65 00 00 00	OatAFVzm15.exe	success or wait	36	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	5732	752	00 00 fd 6f 00 00 00 00 00 60 2e 00 fd 08 2e 00 fd fd 44 68 1d 00 00 fd 04 fd fd 00 00 01 00 00 00 0b 00 01 00 fd 42 00 00 0b 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 10 fd 02 00 00 00 00 49 3c 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 7a 7e 03 00 00 00 00 00 7a 7e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 5a 1b 00 00 00 00 00 6f fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 0b fd 04 00 00 00 00	o`..hBB? $@AZbl<z~z~Zo@	success or wait	1	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	31252	3464	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8AB9.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 34 0f 00 00 fd 07 00 00 05 00 00 00 14 01 00 00 fd 28 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 08 00 00 1c 7f 00 00 15 00 00 00 fd 01 00 00 fd 16 00 00 16 00 00 00 fd 00 00 00 fd 18 00 00	4(T8T	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.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	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	964	28	3c 00 50 00 69 00 64 00 3e 00 37 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>772</Pid>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	992	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	996	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1000	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 4f 00 61 00 74 00 41 00 46 00 56 00 7a 00 6d 00 31 00 35 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>OatAFVzm15.exe</ImageName>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1082	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1180	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 35 00 39 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>3599</Uptime>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1230	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1320	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1380	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1434	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 36 00 30 00 39 00 31 00 39 00 38 00 30 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>60919808</PeakVirtualSize>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1530	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 36 00 30 00 39 00 31 00 31 00 36 00 31 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>60911616</VirtualSize>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1610	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 33 00 36 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1365</PageFaultCount>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1694	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 30 00 35 00 30 00 33 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>5050368</PeakWorkingSetSize>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1800	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 30 00 35 00 30 00 33 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>5050368</WorkingSetSize>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	1890	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 37 00 32 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>112720</QuotaPeakPagedPoolUsage>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 37 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>112720</QuotaPagedPoolUsage>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 39 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 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>16960</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 36 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>16608</QuotaNonPagedPoolUsage>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2374	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 34 00 31 00 37 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1441792</PagefileUsage>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2460	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 34 00 39 00 39 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1449984</PeakPagefileUsage>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2562	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 34 00 31 00 37 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1441792</PrivateUsage>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2642	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2696	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2736	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2788	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2830	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	2912	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 36 00 37 00 31 00 35 00 31 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5671519</Uptime>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3074	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3164	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3228	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3286	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3390	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3478	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 31 00 38 00 33 00 32 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>61832</PageFaultCount>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 36 00 35 00 30 00 30 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>123650048</PeakWorkingSetSize>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3682	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 32 00 37 00 30 00 33 00 38 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>122703872</WorkingSetSize>	success or wait	1	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3780	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 34 00 32 00 39 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>1142952</QuotaPeakPagedPoolUsage>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3896	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3900	2	09 00		success or wait	5	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	3910	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 38 00 35 00 35 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1085552</QuotaPagedPoolUsage>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4024	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4148	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4152	2	09 00		success or wait	5	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4162	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 30 00 32 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>80240</QuotaNonPagedPoolUsage>	success or wait	1	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4284	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 36 00 33 00 39 00 31 00 32 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>46391296</PagefileUsage>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4376	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 38 00 35 00 31 00 37 00 31 00 32 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>48517120</PeakPagefileUsage>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4470	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4474	2	09 00		success or wait	5	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4484	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 36 00 33 00 39 00 31 00 32 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>46391296</PrivateUsage>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4558	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4562	2	09 00		success or wait	4	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4570	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	3	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4626	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	2	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4676	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4714	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4762	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4800	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4804	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4808	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4870	4	0d 00 0a 00		success or wait	8	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4874	2	09 00		success or wait	16	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	4878	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 4f 00 61 00 74 00 41 00 46 00 56 00 7a 00 6d 00 31 00 35 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>OatAFVzm15.exe</Parameter0>	success or wait	8	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	5482	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	5486	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	5488	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	5528	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	5532	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	5534	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	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	5572	4	0d 00 0a 00		success or wait	6	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	5576	2	09 00		success or wait	12	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	5580	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6134	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6138	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6140	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6180	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6184	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6186	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6224	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6228	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6232	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6326	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6330	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6334	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 71 00 68 00 70 00 78 00 6f 00 75 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>qhpxou, Inc.</SystemManufacturer>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6440	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6444	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6448	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 71 00 68 00 70 00 78 00 6f 00 75 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>qhpxou7,1</SystemProductName>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6544	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6548	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6552	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6672	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6676	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6680	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 30 00 30 00 31 00 33 00 37 00 37 00 35 00 32 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>1600137752</OSInstallDate>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6762	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6766	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6770	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6872	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6876	2	09 00		success or wait	2	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6880	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6948	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6952	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6954	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6994	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	6998	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7000	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7034	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7038	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7042	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7138	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7142	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7144	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7186	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7210	4	0d 00 0a 00		success or wait	3	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7214	2	09 00		success or wait	6	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7218	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 32 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000002</Flags>	success or wait	3	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7464	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7468	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7470	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7496	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7500	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7502	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 38 00 2d 00 32 00 37 00 54 00 31 00 30 00 3a 00 35 00 39 00 3a 00 35 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-08-27T10:59:51Z">	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7602	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7606	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7610	256	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 32 00 39 00 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 37 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 38 00 31 00 32 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 38 00 31 00 32 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22 00 3e	<Process AsId="293" PID="772" UptimeMS="812" TimeSinceCreationMS="812" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1">	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7866	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7870	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7874	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	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7894	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7898	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7900	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7944	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7982	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7986	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	7990	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 34 00 61 00 65 00 66 00 61 00 35 00 64 00 2d 00 33 00 30 00 64 00 39 00 2d 00 34 00 35 00 33 00 30 00 2d 00 38 00 34 00 39 00 36 00 2d 00 65 00 39 00 33 00 36 00 66 00 33 00 33 00 66 00 32 00 35 00 62 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>d4aefa5d-30d9-4530-8496-e936f33f25b9</Guid>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	8088	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	8092	2	09 00		success or wait	2	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	8096	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 38 00 2d 00 32 00 37 00 54 00 31 00 30 00 3a 00 35 00 39 00 3a 00 35 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-08-27T10:59:51Z</CreationTime>	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	8194	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	8198	2	09 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	8200	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	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	8240	4	0d 00 0a 00		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E06.tmp.WERInternalMetadata.xml	8244	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	6D4C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.xml	0	4567	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_OatAFVzm15.exe_a26318744316683b0d1fe53934c2b47109f797_532d33bc_179a95d5\Report.wer	0	2	fd fd		success or wait	1	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_OatAFVzm15.exe_a26318744316683b0d1fe53934c2b47109f797_532d33bc_179a95d5\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	161	6D4C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_OatAFVzm15.exe_a26318744316683b0d1fe53934c2b47109f797_532d33bc_179a95d5\Report.wer	10478	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 34 00 39 00 38 00 35 00 39 00 34 00 39 00 36 00 34 00	MetadataHash=-498594964	success or wait	1	6D4C497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	success or wait	1	6D4E36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D4E1FB2	RegCreateKeyExW
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D4C43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	ProgramId	unicode	0006576f609710f3cdf063577dc7a58c7ece0000ffff	success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	FileId	unicode	00004affabf1f09e55a1777fedbe83fc26905943045c	success or wait	1	6D4E36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	LowerCaseLongPath	unicode	c:\users\user\desktop\oatafvzm15.exe	success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	LongPathHash	unicode	oatafvzm15.exe\77839bf3	success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	Name	unicode	oatafvzm15.exe	success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	Publisher	unicode		success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	Version	unicode		success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	BinFileVersion	unicode		success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	BinaryType	unicode	pe32_i386	success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	ProductName	unicode		success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	ProductVersion	unicode		success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	LinkDate	unicode	04/28/2004 18:04:37	success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	BinProductVersion	unicode		success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	Size	B	00 14 04 00 00 00 00 00	success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	Language	dword	0	success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	IsPeFile	dword	1	success or wait	1	6D4E36BF	unknown
\REGISTRY\A\{522e3623-668e-c9a3-6fdc-8b4048ff1dbe}\Root\InventoryApplicationFile\oatafvzm15.exe\77839bf3	IsOsComponent	dword	0	success or wait	1	6D4E36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 D9 E7 8B 77 02 00 00 00 01 00 00 00 00 10 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6D4E1FE8	RegSetValueExW

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

Disassembly

No disassembly