ID: 756303
Sample Name: file.exe
Cookbook: default.jbs
Time: 00:22:09
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

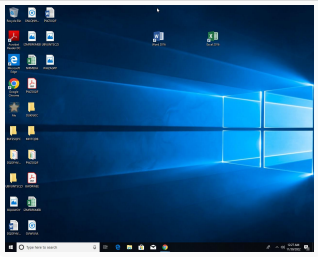
Windows Analysis Report

file.exe

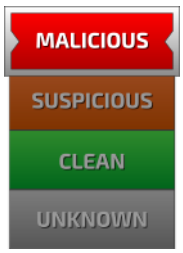
Overview

General Information

Sample Name:	file.exe
Analysis ID:	756303
MD5:	2479739c5d062e..
SHA1:	4394b6d2ca4ed8..
SHA256:	728de9789af5f2e.
Tags:	exe
Infos:	



Detection

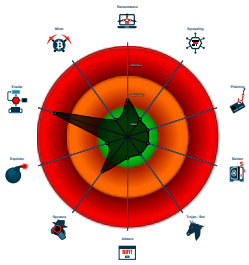


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Detected unpacking (changes PE se…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Tries to detect virtualization through…
- Machine Learning detection for sam…
- Creates a DirectInput object (often f…
- Uses 32bit PE files
- AV process strings found (often use…
- Yara signature match
- One or more processes crash
- Extensive use of GetProcAddress (…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 3548 cmdline: C:\Users\user\Desktop\file.exe MD5: 2479739C5D062ECB325147623241F007)
  - rundll32.exe (PID: 5248 cmdline: C:\Windows\system32\rundll32.exe C:\Users\user\AppData\Local\Temp\Serpodtudpwhhta.dll,start MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5412 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5248 -s 668 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.258419981.0000000002766000.00000040.00000800.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x798:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000000.00000002.260555630.0000000002AF0000.00000040.00000001.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
Process Memory Space: file.exe PID: 3548	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion

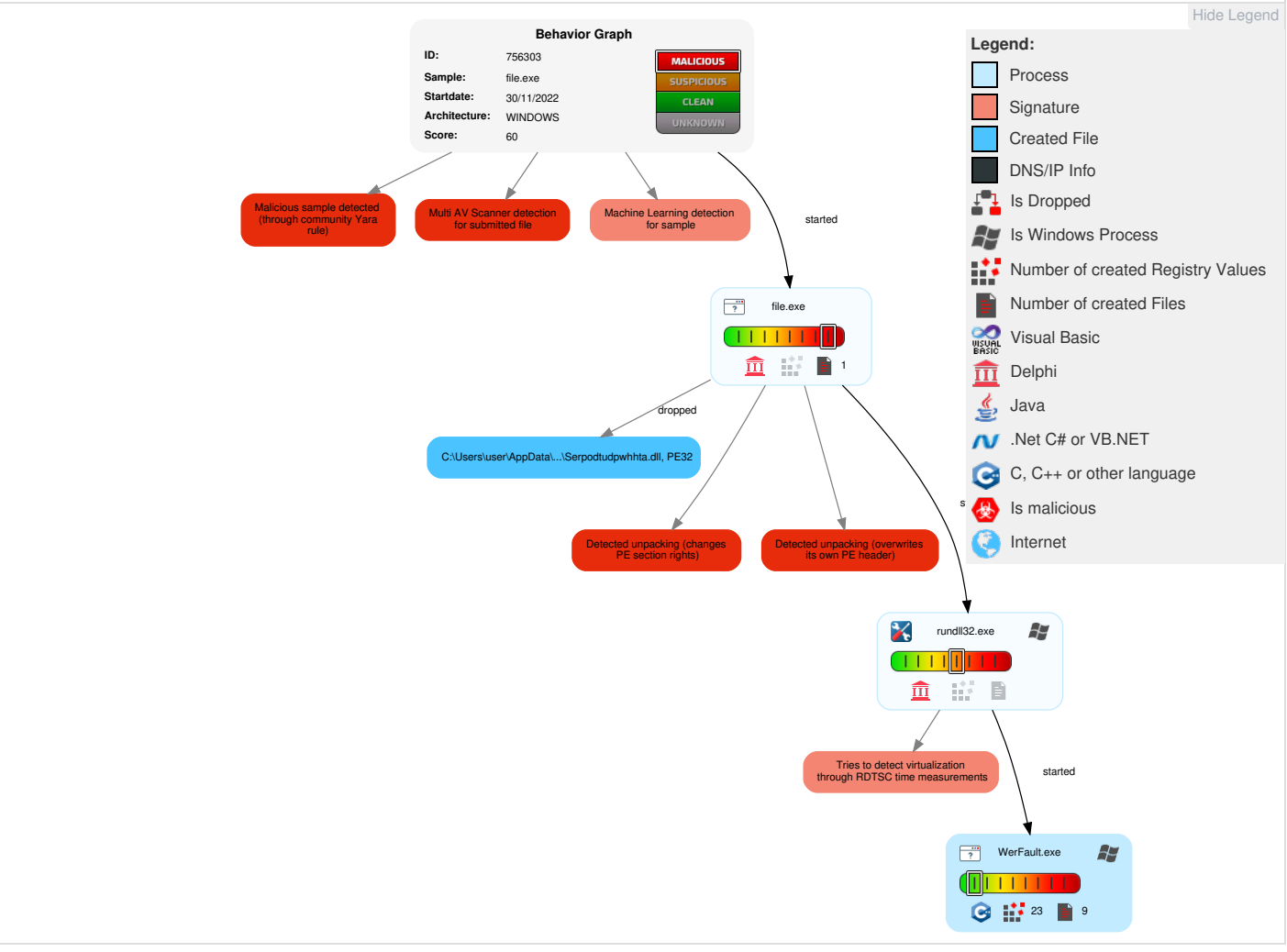
Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	1 Process Injection	1 Virtualization/Sandbox Evasion	1 Input Capture	1 2 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 Process 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)	2 Obfuscated Files or Information	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Rundll32	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Software Packing	Cached Domain Credentials	1 1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

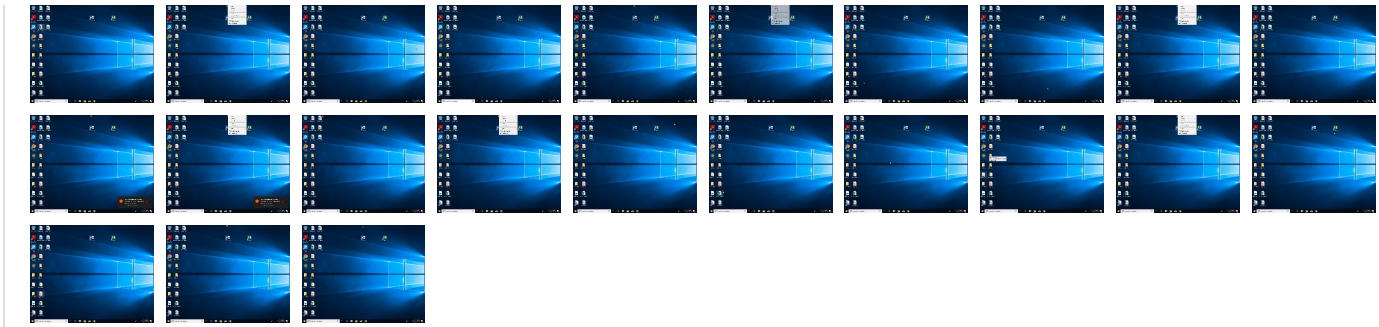
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
file.exe	39%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756303
Start date and time:	2022-11-30 00:22:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.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
Number of analysed new started processes analysed:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.evad.winEXE@4/5@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.4%) • Quality average: 77.5% • Quality standard deviation: 0.5%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.21

- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus16.westus.cloudapp.azure.com, ctldl.windowsupdate.com, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
00:23:18	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c7d966c262eae458e8625727f886cf5c34890_82810a17_156d127b\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9485641811025363
Encrypted:	false
SSDEEP:	192:p6lia0oXaHqqBIKjed+Mb/u7sqS274ItWc:0liMXyqqBIKjet/u7sqX4ItWc
MD5:	86B4D7D5A7632D224C45634319F9DDCF
SHA1:	4C72DCDB359F85A40C573C9F8B21E6D918E66635
SHA-256:	76A197B110567751607902657F4C8C73EAE08E9A5F40C3E6A5BDB4B56F6C8352
SHA-512:	9F842FC1D5724DB0F20F7C788A0E79991F1AEA19FCFC8322A379FF7BC6A562B828A5683B4F1CD68965EB0D74C27C0829EBEAD0AB8C35824E36E5014A6A17FE A
Malicious:	false
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.=.1.3.3.1.4.2.7.0.1.9.3.0.7.1.0.7.4.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.1.4.2.7.0.1.9.4.6.6.4.8.3.4.2.....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.=.2.0.4.2.6.8.1.d.-.9.d.a.2.-.4.c.6.f.-.b.3.6.1.-.c.0.5.0.f.3.9.1.9.a.3.a.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.3.1.4.6.1.1.0.-.c.b.2.6.-.4.5.1.d.-.9.b.8.b.-.4.c.8.9.9.f.4.6.2.3.b.9.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.8.0.-.0.0.0.1.-.0.0.1.a.-.b.f.3.9.-.d.1.f.9.9.4.0.4.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AE.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4640
Entropy (8bit):	4.463699038830804
Encrypted:	false
SSDEEP:	48:cvIwSD8zs7JgtWI9rjWgc8sqYj28fm8M4JCdsFIAaFov+q8/RgEAR4SrSz6d:uITfVISgrsqYnJvIuvE1MDWz6d
MD5:	CD2574D210A7A42D1B4B2DCA3FC3D1C1
SHA1:	02000F08ADFB84655075CFFB69B6A9CB52C2A03C
SHA-256:	BC8C2BE9F9D1DB01049430C046927F5450F9E24E957B336F22CBE5021436A9C3
SHA-512:	7C865D49D91C1BB8568FCAA5D6CC7150789E676358A38D86C937787EFF463765A80FFC72C4A2FF6D67C5819C7333C8376DDAB081789119D4A7527D677304937(
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="1802493" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	6306
Entropy (8bit):	3.713455556373279
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNimP6ALa0ZDYTMSmGCprY89bxGKsfTUzcm:RrlsNiO6SaIDYTMSmbxGpfT6p
MD5:	BBBE86D86C59A9FFB64F22071FEDA7CA
SHA1:	09E81EF93A62EF6326ADF10B6E1B62BDC047B407
SHA-256:	199C6EA74D0B7C9B08E055E4E0B1B27BFEB213ECF41EF3473659F414199C92C8
SHA-512:	25CA4D998F69F01D0712C7C904545D27E748FECEFE260F84EEBD955562BB3D779F61E2A5CD6165E2A7358801CE319F1A281DF5FBEB96F719CE250E99AB46A13E
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.>.5.2.4.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Nov 30 08:23:13 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	47656
Entropy (8bit):	2.1094804680206685
Encrypted:	false
SSDEEP:	192:YpvotW/mZyO5SkbDV8+T1szomNet4r5j3Hl1NqwWk:ae5LbZ8+T1bceAZ3hck
MD5:	B8F33F0009F3DDE318CB9B992C517AEB
SHA1:	05A2D6FAEAF1B9A1D05959641B7871480F8782C2
SHA-256:	7EAE34186E263D33DD21713C8D48A45FFC0BC5D9D75AF9D5A71AF52B677F5730
SHA-512:	04EF2D049D1D9D3678A14FCA62435B725EA9A79E264A56866F2B7A9C88DDDC122A5AB754F75F1CA262CDF2C38A8D7CE4E53F3C24671B5FC81251B656774D7C1
Malicious:	false

Reputation:	low
Preview:	MDMP..... .....c.....D...../.....T.....8.....T.....U.....B.....d.....GenuineIntelW.....T.....c.....0..1.....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:\Users\user\AppData\Local\Temp\Serpodtudpwhhta.dll	
Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4494336
Entropy (8bit):	6.573454988842364
Encrypted:	false
SSDEEP:	98304:2Ekp3AUUgGFofLw++PxAbc5rh5Ar/04TAYP:gp31UtFmLw95Abc5rh5Ar/NTA
MD5:	3D3D6C4F7A605B366E27DAA16D5C50F5
SHA1:	78B8FE5C09838213D0A8B1A4D4FF727C989D2AD2
SHA-256:	011D953568F11D2DC9752807D15F50144DF7D5D4277B19278477B6AC7F920804
SHA-512:	3AD1AA5FBA5BD1D45FBAC6BB4D40B6CF59B45F2C6CA5F8BCC90BA1FB16042D8D7804A96FD9738FE320E13508E623B79DE149E2F5745E8E363301E9DB119CBD20
Malicious:	false
Reputation:	low
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....PE..L.....c.....?.....X&?.....0?...@.....pE.....@.....@@..9....E..d.....@.4A.....J@.....@.....text.....>.....>..... ..`.itext..t.....?.....>..... ..`.data.....0?.....?.....@....bss....Tg....?.....idata...9...@@..:....?.....@....didata.....@.....?.....@....edata.....@.....?.....@..@.rdata..D.....@.....?.....@..@.reloc..4A....@..B....?.....@..B.rsrc....d....E..d...0D.....@..@.....pE.....D.....@..@.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.994112157171111
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	3776000
MD5:	2479739c5d062ecb325147623241f007
SHA1:	4394b6d2ca4ed82a5f2d70d10cd05cfa3b35ab2c
SHA256:	728de9789af5f2ebc9ac2fac80fee25b186bc5b3acb960650934377f0c77726d
SHA512:	1c5c4d7d7fd5a7f18fed87a0d66b95b26ebfda33b4aa4f66fd8fd4432e07ebc6e6289a27ffccc1cf99e659aeb80434e833baa299ab140d82c0bcb7d863a58301
SSDEEP:	98304:CIPeMtJl37YfXo0/PrjRkwoD8sOr+616vbgD7op:CIPeMh37YfXZPvRkww3OrNEgo
TLSH:	C9063396722288F5C386833C17D0F1306D7F78936A514947F7E42A2CC77A5DAE668F48
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q.'.5.I.5.I.5.I.....4.I.+...$.I.+...].I..]2.2.I.5.H...I.+.....I.+...4.I.+...4.I.Rich5.I.....PE..L.....`.....

File Icon

Icon Hash:	d4b4b0e0f0eaf0c0

Static PE Info

General

Entrypoint:	0x404c97
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x60E5ACA2 [Wed Jul 7 13:31:14 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	2ac0f7085258eff31142b9f87cb0f218

Entrypoint Preview
Instruction
call 00007F93209C0D2Ch
jmp 00007F93209BAF0Dh
sub eax, 000003A4h
je 00007F93209BB0B4h
sub eax, 04h
je 00007F93209BB0A9h
sub eax, 0Dh
je 00007F93209BB09Eh
dec eax
je 00007F93209BB095h
xor eax, eax
ret
mov eax, 00000404h
ret
mov eax, 00000412h
ret
mov eax, 00000804h
ret
mov eax, 00000411h
ret
mov edi, edi
push esi
push edi
mov esi, eax
push 00000101h
xor edi, edi
lea eax, dword ptr [esi+1Ch]
push edi
push eax
call 00007F93209BC29Eh
xor eax, eax
movzx ecx, ax
mov eax, ecx
mov dword ptr [esi+04h], edi
mov dword ptr [esi+08h], edi
mov dword ptr [esi+0Ch], edi
shl ecx, 10h
or eax, ecx
lea edi, dword ptr [esi+10h]
stosd
stosd
stosd
mov ecx, 00796ED8h
add esp, 0Ch

Instruction
lea eax, dword ptr [esi+1Ch]
sub ecx, esi
mov edi, 00000101h
mov dl, byte ptr [ecx+eax]
mov byte ptr [eax], dl
inc eax
dec edi
jne 00007F93209BB089h
lea eax, dword ptr [esi+0000011Dh]
mov esi, 00000100h
mov dl, byte ptr [eax+ecx]
mov byte ptr [eax], dl
inc eax
dec esi
jne 00007F93209BB089h
pop edi
pop esi
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 0000051Ch
mov eax, dword ptr [00797AE0h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
push edi
lea eax, dword ptr [ebp-00000518h]
push eax
push dword ptr [esi+04h]
call dword ptr [00401170h]
mov edi, 00000100h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10a9c	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3cc000	0x3050	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1280	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x2d20	0x18	.text
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2cd8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x23c	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x107d4	0x10800	False	0.5123106060606061	data	6.1122560152151895	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x12000	0x3b9788	0x386000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3cc000	0x125050	0x3200	False	0.62890625	data	5.650799726445505	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
JEBOPOZUSUHARAFA	0x3ce430	0x55f	ASCII text, with very long lines (1375), with no line terminators	Raeto-Romance	Switzerland
RT_ICON	0x3cc2b0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x3cc978	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x3ccee0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x3cdf88	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Raeto-Romance	Switzerland
RT_STRING	0x3ceb78	0x2d8	data	Raeto-Romance	Switzerland
RT_STRING	0x3cee50	0x1fc	data	Raeto-Romance	Switzerland
RT_ACCELERATOR	0x3ce990	0xa0	data	Raeto-Romance	Switzerland
RT_GROUP_ICON	0x3ce3f0	0x3e	data	Raeto-Romance	Switzerland
RT_VERSION	0x3cea30	0x148	x86 executable not stripped		

Imports

DLL	Import
KERNEL32.dll	OpenMutexW, GetConsoleAliasExesLengthA, CopyFileExA, ReadConsoleOutputCharacterW, CompareStringW, SetVolumeLabelA, FillConsoleOutputAttribute, GetConsoleTitleA, QueryDosDeviceW, EnumCalendarInfoExA, GetProcessPriorityBoost, IsProcessInJob, AddConsoleAliasW, CreateFileW, SetMailslotInfo, GetWindowsDirectoryW, GetModuleHandleA, GlobalLock, CreateDirectoryExW, GetLogicalDriveStringsA, ReadConsoleInputA, FindNextVolumeMountPointW, OpenWaitableTimerA, GetVersionExA, SearchPathA, MoveFileExW, CallNamedPipeW, GetCurrentDirectoryW, GetDriveTypeA, CreateMailslotA, BuildCommDCBAndTimeoutsA, GetProcAddress, LoadLibraryA, LocalAlloc, GetBinaryTypeA, GetCPInfoExW, WriteConsoleOutputA, GetCommandLineA, EnumDateFormatsW, CancelTimerQueueTimer, GetHandleInformation, FindResourceA, CreateJobObjectA, FindFirstVolumeA, GlobalFlags, CreateNamedPipeW, InterlockedIncrement, CloseHandle, CopyFileW, GetComputerNameExA, GetShortPathNameA, FlushFileBuffers, GetLogicalDriveStringsW, InterlockedCompareExchange, EnumCalendarInfoW, GetConsoleAliasExesLengthW, InterlockedExchange, GetNamedPipeHandleStateW, GetModuleHandleW, GetCurrentActCtx, GenerateConsoleCtrlEvent, MoveFileW, AddAtomA, SetThreadPriority, FreeEnvironmentStringsW, SetConsoleTitleW, SetVolumeMountPointW, VirtualAlloc, _hread, EnumResourceLanguagesW, ClearCommBreak, QueryMemoryResourceNotification, GlobalFindAtomA, HeapWalk, SetFilePointer, GetTickCount, EnumSystemCodePagesW, VerifyVersionInfoA, LoadLibraryW, CreateFileA, GetLastError, WideCharToMultiByte, HeapReAlloc, HeapAlloc, HeapFree, UnhandledExceptionFilter, SetUnhandledExceptionFilter, DeleteFileA, GetStartupInfoA, GetCPInfo, InterlockedDecrement, GetACP, GetOEMCP, IsValidCodePage, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetCurrentThreadId, TerminateProcess, GetCurrentProcess, IsDebuggerPresent, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, HeapCreate, VirtualFree, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, GetEnvironmentStringsW, SetHandleCount, GetFileType, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, SetStdHandle, GetConsoleCP, GetConsoleMode, RtlUnwind, InitializeCriticalSectionAndSpinCount, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, HeapSize, ReadFile
GDI32.dll	GetCharWidthA, GetCharABCWidthsA
WINHTTP.dll	WinHttpSetOption

Possible Origin

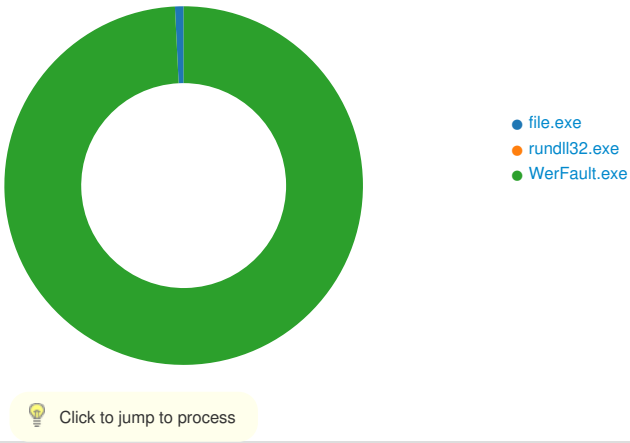
Language of compilation system	Country where language is spoken	Map
Raeto-Romance	Switzerland	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 3548, Parent PID: 3452

General

Target ID:	0
Start time:	00:22:59
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	3776000 bytes
MD5 hash:	2479739C5D062ECB325147623241F007
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.258419981.0000000002766000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.260555630.0000000002AF0000.00000040.00000001.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: rundll32.exe PID: 5248, Parent PID: 3548

General

Target ID:	1
Start time:	00:23:07
Start date:	30/11/2022

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\rundll32.exe C:\Users\user\AppData\Local\Temp\Serpodtudpwhhta.dll,start
Imagebase:	0x80000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **5412**, Parent PID: **5248**

General

Target ID:	3
Start time:	00:23:12
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5248 -s 668
Imagebase:	0x8c0000
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	6D831717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AE.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D82497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c7d966c262eae458e8625727f886cf5c34890_82810a17_156d127b	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c7d966c262eae458e8625727f886cf5c34890_82810a17_156d127b\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D82497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AE.tmp	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AE.tmp.xml	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE452.tmp.csv	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE472.tmp.txt	success or wait	1	6D82497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 12 fd 63 fd 05 12 00 00 00 00 00	MDMP c	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	7780	6	00 00 00 00 00 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.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 64 1e 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 14 00 00 fd 12 fd 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 31 00 00 00 00 00 00 00 01 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UBdGenuineIntelWTc01Pacific Standard TimePacific Daylight Time	success or wait	1	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	9190	716	fd fd 16 02 fd fd fd 03 fd fd 16 02 56 fd fd 77 fd fd 16 02 94 fd 77 00 00 fd 03 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2d 62 fd fd 0c 5d 02 08 fd 5c 02 fd 0c 5d 02 24 00 00 00 01 00 00 00 fd 00 5e 02 fd fd 5d 02 30 00 00 00 07 fd fd fd 53 00 fd fd fd 7c fd 77 00 00 00 00 08 fd 5c 02 08 fd 5c 02 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	Vww-]\]$^]0S|w\\	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	1620	168	7c 14 00 00 00 00 00 00 fd 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 3e fd 2a 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 23 00 00	|>*#	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	12054	20	0e 00 00 00 fd fd 5c 02 00 00 00 00 04 00 00 00 fd 2f 00 00	\/	success or wait	14	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	12282	4	1c fd 56 02	V	success or wait	13	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	35990	1968	fd fd fd 77 fd fd fd 77 50 02 00 00 fd fd fd fd 10 00 00 00 fd fd 56 02 fd fd 56 02 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd 00 fd 2e 02 00 fd 2e 02 00 00 00 00 50 02 00 00 fd fd fd fd 50 02 00 00 fd fd fd fd 00 fd 2e 02 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 06 5d 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd 5c 02 00 00 00 00 00 00 00 00 fd 08 5d 02 00 40 2e 02 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 02 54 42 2e 02 fd fd fd 02 28 07 5d 02 00 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	wwPVV@w@w..PP.]\]@.TB.(]	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	9906	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 16 02 fd fd fd 77 23 00 00 00 16 02 20 00 fd fd 16 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w# +	success or wait	3	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	1888	48	48 14 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 2e 02 00 00 00 00 20 fd fd 02 00 00 00 00 fd 06 00 00 fd 67 00 00 fd 02 00 00 4a 2c 00 00	H . gJ,	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	1948	4	30 00 00 00	0	success or wait	48	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	7786	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	48	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	7028	752	00 00 fd 73 00 00 00 00 00 fd 07 00 fd 7b 07 00 5a 14 fd 4f fd 23 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd 02 00 00 00 00 00 30 23 03 00 00 00 00 fd 50 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 5b fd 03 00 00 00 00 00 5c fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 6c 50 1b 00 00 00 00 00 2e 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 5b fd 04 00 00 00 00	s{ZO#BB? %@AZb0#P[\lP@[	success or wait	1	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	37958	9698	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE66.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 44 14 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 16 2f 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 1a 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 1b 00 00 16 00 00 00 fd 00 00 00 fd 1d 00 00	D/T8T	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.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	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 32 00 34 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5248</Pid>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 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>rundll32.exe</ImageName>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1080	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 32 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>00000002</CmdLineSignature>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 30 00 36 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6069</Uptime>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1228	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1318	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1378	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 30 00 38 00 36 00 33 00 31 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>130863104</PeakVirtualSize>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 30 00 36 00 37 00 34 00 36 00 38 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>130674688</VirtualSize>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 30 00 35 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>4057</PageFaultCount>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1696	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 34 00 32 00 32 00 30 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>14422016</PeakWorkingSetSize>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1794	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1798	2	09 00		success or wait	3	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1804	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 34 00 32 00 32 00 30 00 31 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>14422016</WorkingSetSize>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1886	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1890	2	09 00		success or wait	3	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	1896	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 38 00 38 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>188800</QuotaPeakPagedPoolUsage>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2010	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2014	2	09 00		success or wait	3	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2020	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 38 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>188584</QuotaPagedPoolUsage>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2118	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2122	2	09 00		success or wait	3	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2128	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 39 00 34 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>59400</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2252	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2256	2	09 00		success or wait	3	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2262	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 39 00 30 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>59048</QuotaNonPagedPoolUsage>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2370	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2374	2	09 00		success or wait	3	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2380	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 38 00 34 00 32 00 31 00 31 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>10842112</PagefileUsage>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2458	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2462	2	09 00		success or wait	3	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2468	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 38 00 35 00 30 00 33 00 30 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>10850304</PeakPagefileUsage>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2562	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2566	2	09 00		success or wait	3	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2572	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 38 00 34 00 32 00 31 00 31 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>10842112</PrivateUsage>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2646	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2650	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2654	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2700	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2704	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2706	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2748	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2752	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2754	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2792	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2796	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2800	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2862	4	0d 00 0a 00		success or wait	8	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2866	2	09 00		success or wait	16	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	2870	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 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>rundll32.exe</Parameter0>	success or wait	8	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	3490	4	0d 00 0a 00		success or wait	1	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	3494	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	3496	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	3536	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	3540	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	3542	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	3580	4	0d 00 0a 00		success or wait	6	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	3584	2	09 00		success or wait	12	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	3588	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4148	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4188	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4192	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4194	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4232	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4236	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4240	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4334	4	0d 00 0a 00		success or wait	1	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4338	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4342	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 67 00 68 00 62 00 6b 00 77 00 73 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>ghbkws, Inc.</SystemManufacturer>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4448	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4452	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4456	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 67 00 68 00 62 00 6b 00 77 00 73 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>ghbkws7,1</SystemProductName>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4560	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4680	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4684	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4688	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 31 00 39 00 31 00 36 00 38 00 38 00 37 00 34 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>1619168874</OSInstallDate>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4770	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4774	2	09 00		success or wait	2	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4778	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4880	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4884	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4888	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4956	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4960	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	4962	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5002	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5006	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5008	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5042	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5046	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5050	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5146	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5150	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5152	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	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5188	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5192	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5194	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5218	4	0d 00 0a 00		success or wait	3	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5222	2	09 00		success or wait	6	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5226	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5484	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5488	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5490	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5516	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5520	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5522	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 31 00 31 00 2d 00 33 00 30 00 54 00 30 00 38 00 3a 00 32 00 33 00 3a 00 31 00 33 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-30T08:23:13Z">	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5622	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5626	2	09 00		success or wait	2	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5630	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 32 00 34 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 38 00 37 00 35 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 37 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="302" PID="5248" UptimeMS="875" TimeSinceCreationMS="875" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5888	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5892	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5896	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5916	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5920	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5922	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5960	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5964	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	5966	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	6004	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	6008	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	6012	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 30 00 34 00 32 00 36 00 38 00 31 00 64 00 2d 00 39 00 64 00 61 00 32 00 2d 00 34 00 63 00 36 00 66 00 2d 00 62 00 33 00 36 00 31 00 2d 00 63 00 30 00 35 00 30 00 66 00 33 00 39 00 31 00 39 00 61 00 33 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>2042681d-9da2-4c6f-b361-c050f3919a3a</Guid>	success or wait	1	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	6110	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	6114	2	09 00		success or wait	2	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	6118	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 31 00 31 00 2d 00 33 00 30 00 54 00 30 00 38 00 3a 00 32 00 33 00 3a 00 31 00 33 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-11-30T08:23:13Z</CreationTime>	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	6216	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	6220	2	09 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	6222	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	6262	4	0d 00 0a 00		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE8.tmp.WERInternalMetadata.xml	6266	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	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2AE.tmp.xml	0	4640	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c7d966c262eae458e8625727f886cf5c34890_82810a17_156d127b\Report.wer	0	2	fd fd		success or wait	1	6D82497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c7d966c262eae458e8625727f886cf5c34890_82810a17_156d127b\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	174	6D82497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c7d966c262eae458e8625727f886cf5c34890_82810a17_156d127b\Report.wer	11964	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 37 00 35 00 34 00 32 00 31 00 30 00 37 00 31 00 33 00	MetadataHash=-1754210713	success or wait	1	6D82497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6D8436BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D841FB2	RegCreateKeyExW
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D8243D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LongPathHash	unicode	rundll32.exe\ab97b57a	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6D8436BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6D8436BF	unknown
\REGISTRY\A\{a7e87e7e-0e87-aa13-b82e-565665afc261}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6D8436BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	96 00 00 C0 00 00 00 00 00 00 00 00 3E 84 2A 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6D841FE8	RegSetValueExW

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

Disassembly

No disassembly