ID: 828171
Sample Name: unpacked (1).dll
Cookbook: default.jbs
Time: 20:01:31
Date: 16/03/2023
Version: 37.0.0 Beryl

Table of Contents

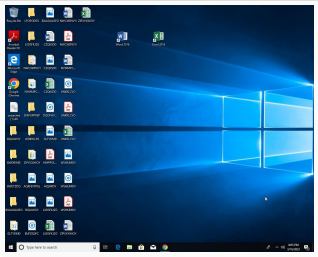
Windows Analysis Report

unpacked (1).dll

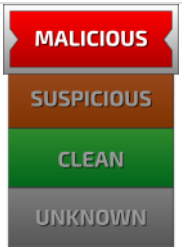
Overview

General Information

Sample Name:	unpacked (1).dll
Original Sample Name:	unpacked (1).bin
Analysis ID:	828171
MD5:	895004ddaa37…
SHA1:	0fb1a2c065131..
SHA256:	74ef237a5145c..
Infos:	



Detection



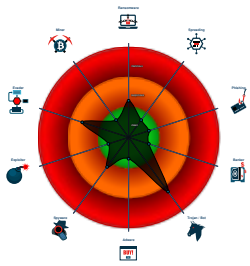
Ursnif

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Machine Learning detection for sam…
- Creates a DirectInput object (often f…
- Uses 32bit PE files
- AV process strings found (often use…
- PE file does not import any functions
- Antivirus or Machine Learning detec…
- One or more processes crash
- Uses code obfuscation techniques (…
- Checks if the current process is bei…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5984 cmdline: loaddll32.exe "C:\Users\user\Desktop\unpacked (1).dll" MD5: 1F562FBF37040EC6C43C8D5EF619EA39)
  - conhost.exe (PID: 5980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6032 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\unpacked (1).dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6092 cmdline: rundll32.exe "C:\Users\user\Desktop\unpacked (1).dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 1236 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6092 -s 636 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Gozi, Ursnif	2000 Ursnif aka Snifula2006 Gozi v1.0, Gozi CRM, CRM, Papras2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*)-> 2010 Gozi Prinimalka -> Vawtrak/NeverquestIn 2006, Gozi v1.0 ('Gozi CRM' aka 'CRM') aka Papras was first observed.It was offered as a CaaS, known as 76Service. This first version of Gozi was developed by Nikita Kurmin, and he borrowed code from Ursnif aka Snifula, a spyware developed by Alexey Ivanov around 2000, and some other kits. Gozi v1.0 thus had a formgrabber module and often is classified as Ursnif aka Snifula.In September 2010, the source code of a particular Gozi CRM dll version was leaked, which led to Vawtrak/Neverquest (in combination with Pony) via Gozi Prinimalka (a slightly modified Gozi v1.0) and Gozi v2.0 (aka 'Gozi ISFB' aka 'ISFB' aka Pandemyia). This version came with a webinject module.	No Attribution	**http://** blog.malwaremustdie.org/2013/02/the-infection-of-styx-exploit-kit.htmlhttp://researchcenter.paloaltonetworks.com/2017/02/unit42-banking-trojans-ursnif-global-distribution-networks-identified/https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/https://blog.gdatasoftware.com/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
unpacked (1).dll	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.loaddll32.exe.10000000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.10000000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	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 Ursnif

E-Banking Fraud

Yara detected Ursnif

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Stealing of Sensitive Information

Yara detected Ursnif

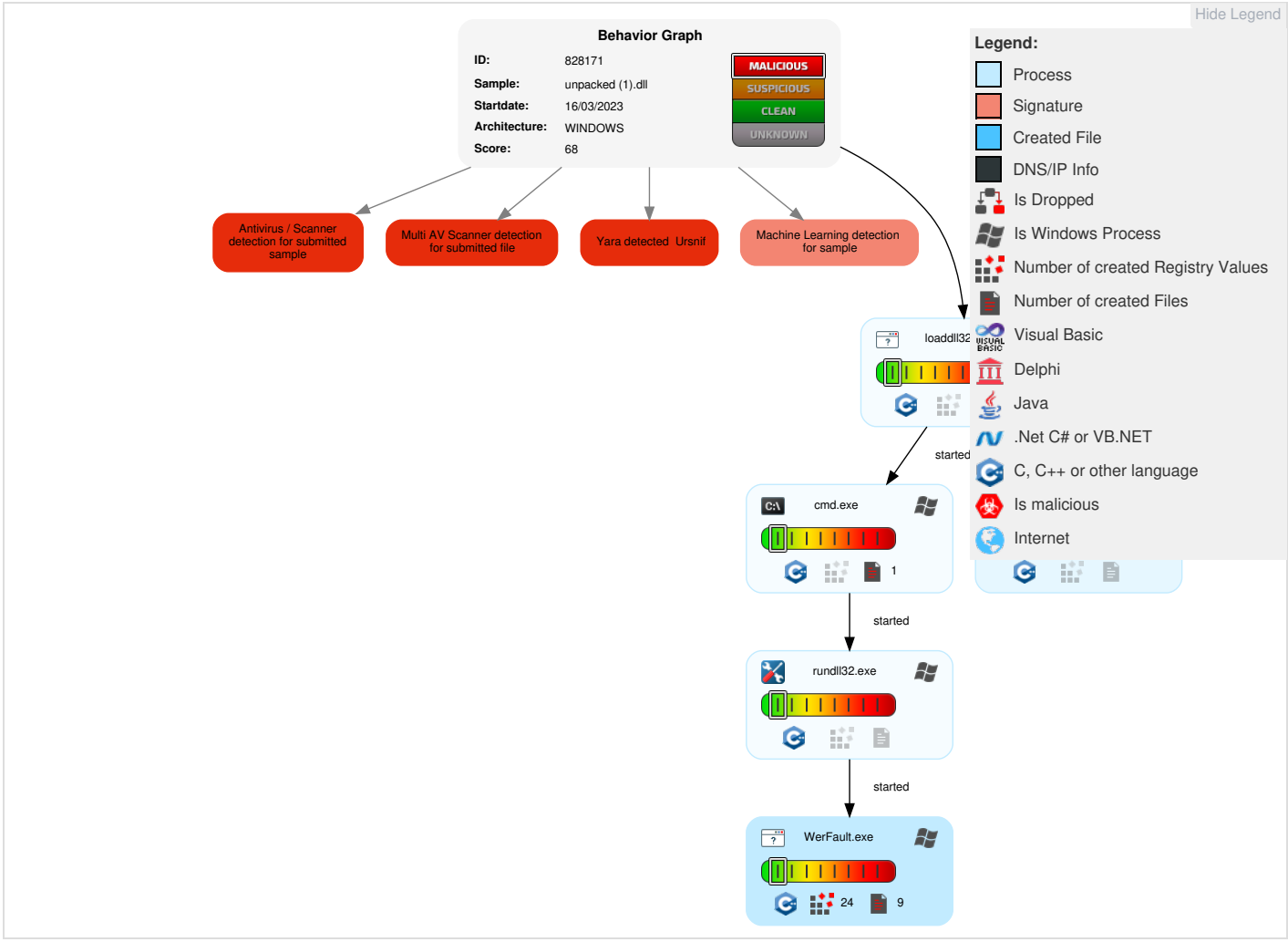
Remote Access Functionality

Yara detected Ursnif

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 1 Process Injection	1 Virtualization/Sandbox Evasion	1 Input Capture	2 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Rundll32	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 Software Packing	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)	1 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

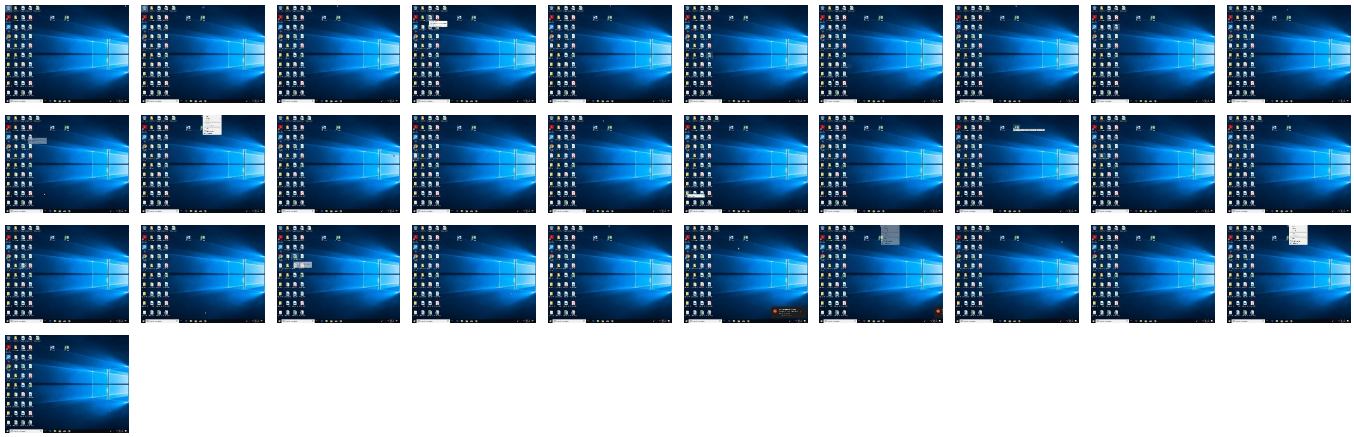
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
unpacked (1).dll	44%	ReversingLabs	Win32.Trojan.Razy	
unpacked (1).dll	100%	Avira	TR/Patched.Ren.Gen2	
unpacked (1).dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.10000000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
3.2.rundll32.exe.10000000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		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://upx.sf.net	Amcache.hve.6.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	828171
Start date and time:	2023-03-16 20:01:31 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	unpacked (1).dll
Original Sample Name:	unpacked (1).bin
Detection:	MAL
Classification:	mal68.troj.winDLL@7/6@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 56% (good quality ratio 34%) • Quality average: 45.1% • Quality standard deviation: 44%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe

- Excluded IPs from analysis (whitelisted): 13.89.179.12
- Excluded domains from analysis (whitelisted): login.live.com, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, onedsblobprdcus17.centralus.cloudapp.azure.com
- Execution Graph export aborted for target loaddll32.exe, PID 5984 because there are no executed function
- Execution Graph export aborted for target rundll32.exe, PID 6092 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: unpacked (1).dll

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_rundll32.exe_7bde5861e98b2ac3cc37e329f3101f62f0fff922_82810a17_049ebf60\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):	0.8868049200890971
Encrypted:	false
SSDEEP:	192:21ApTiH0oXNrHBUZMX4jed+5/u7sgS274ltWc:4ETi5XBBUZMX4jeU/u7sgX4ltWc
MD5:	791B98C1D41CDBB9E8401A80B62072AD
SHA1:	146DB5409523BEBA3953609BA10A1FC53D634E44
SHA-256:	052E7F6D7C5AE8DE41C8C24DAC0AD59884B5FC3150FD68BD83A3A5F3F5D5B075
SHA-512:	E7A66912A2C8D9FB94CCC0F80F3AC423D4C18F227255FE0C01247F601C770E6D1E088DE93D80861F267EC7469461E8B13A0220751203F3B0752F4D8AD2572DA
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.=.1.3.3.2.3.4.6.6.9.4.9.4.0.2.3.0.7.5.....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.=.1.3.3.2.3.4.6.6.9.5.0.1.9.9.1.7.2.4.....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.=.2.7.e.7.8.a.1.5.-.6.9.4.e.-.4.c.8.5.-.b.e.0.6.-.b.5.4.1.3.3.1.3.0.0.1.4.....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.=.a.7.f.8.6.f.e.d.-.f.b.e.e.-.4.3.2.4.-.b.2.a.d.-.5.4.8.6.4.1.6.f.a.b.4.d.....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.=.0.0.0.0.1.7.c.c.-.0.0.0.1.-.0.0.1.f.-.6.5.5.0.-.f.f.d.9.3.9.5.8.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\WER962D.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Mar 16 19:02:29 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	39202
Entropy (8bit):	2.316888820521251
Encrypted:	false
SSDEEP:	192:6nKRf/ecypO5Skb2wrCu7pm8bE+VTiUfCndFGlCPLXHnbxf:yQ5LbG2HDVTYGlCLH
MD5:	0AD73DC60EDD50DB8DDC7FAD8E3F91AE
SHA1:	5553AF467C52AC4EA657C1F253626ADFC4BA278B
SHA-256:	5B0968FE44D3F5C5C78FF317DAB298F7F3BEEB9CB3465F25A0C27C936034E292
SHA-512:	BCD802EFFD600B99C37E789A9714F87B77411C8FE02AB81B35615943B7CE89F9A1F405659A23CD793E9755536A91B0BA7209D424609A98FF532C1B703E4AE38F
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....g.d.....d.....P...l.....^(.....T.....8.....T.....`.....U.....B.....@.....GenuineIntelW.....T.....g.d.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WER97E3.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):	8246
Entropy (8bit):	3.6909810241404664
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiwa6W6Y0m6GgmfTkn4SI+prq89bERsfRsm:RrlsNid6W6Yl6GgmfTk4SXEKfP
MD5:	CD4570E2073BF6C8A1E5705D73EFF621
SHA1:	72171B897357A9F22F439BA595619B4F15D5421D
SHA-256:	CA3CF2DB083B990896C5DFBE1479AF83E327FE91D1CA1C923F037AADA9C608CB
SHA-512:	5843D00BCD0C0B3FB58BA41E72AD765D6900E380E60153A98C293780C84B8A7BBB55E7BF806B2280747AA40F926DA26FAE365DD13760FD8AE8100DB775BB20D8
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.0.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9852.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.455035274816969
Encrypted:	false
SSDEEP:	48:cvIwSD8zshJgtWI959Wgc8sqYjU8fm8M4JCdsfFT+q8/5z04SrS3d:uITfz2MgrsqYVJvzDW3d
MD5:	FF91CF9461FA80350704067CBF0C3B5A
SHA1:	2DC002BB1C23B873D69CA96B9B59075D4F620250
SHA-256:	45A8DE7B90BFE2518B3DCBE949912A316B0EE18CA06572E5FD21AE4EFC14EB52
SHA-512:	E69DF9B30BE9BC15FA7949E8CB3A88CA6D49BFE55E809D57B6DEED6525F6CBE9F802F96F975E4A9DC739474DC9F60F44B352E4D63ABE7959EAEF19C3BFB7EBBA
Malicious:	false

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="1955773" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.310468455996301
Encrypted:	false
SSDEEP:	12288:8Tu4PpvwTNUQz3PUnV9KGSWLE0CLrO83oNl3BHQEF9RO7zQ48y:su4PpvwTNUY3PUyaE6
MD5:	26D44A0A3BCA99378D5E6850CC754389
SHA1:	C35933FB4E53943C040B518B7A639F743280A129
SHA-256:	A6EB65562FBA59BA8BA6C2DC728C029F529AA61148766237BA994DC21370FC92
SHA-512:	F2886BDEC8C62BE832870D4C8850218B87FB80136AEBB660C790176815CA3D5B6FB02D3851DE1B6FF3B923EB057AF1D83E9851B2FC86AE5CFC19D48F336A294B
Malicious:	false
Preview:	regfQ...Q...p.\.,..... ....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E....5.....E.rmtm:.i.9X..... ....C.`.....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.943670216014598
Encrypted:	false
SSDEEP:	384:xHd5K5kjaM1gnVVeeDzeP1NKZtjnexFa1tsoSwXXha4i/qfZ/DWwsfWe0NZpu+:5DKCg/eeDzetNYtjeHaHsoSwha4i/qfO
MD5:	07126390C1555BCC0D8F3498F88C5615
SHA1:	4DCCE05195C761099F1624BC47B7EDB31770D096
SHA-256:	87B5D5E8F05BC3CB7D9B3C88E621FB1C9BE1900923E846A5326C4825610C3BED
SHA-512:	6B64271CE8EA49A2ACD5C92FAD2E4B5927F611A9574241463DF8B156FB1F4F0F16AF89105E6AAB5EA27CCE42955994BE24505237FA423BE1AED9C6A46A3F9E1F
Malicious:	false
Preview:	regfP...P...p.\.,..... ....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E....5.....E.rmtm:.i.9X..... ....E.`.HvLE.^.....P.... .....n.d.FW1.|@t..7X..... ..hbin.....p.\.,.....nk,...l.9X..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ...l.9X..... ....Z.....Root.....lf.....Root....nk ...l.9X..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.765721775191744
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	unpacked (1).dll
File size:	57344
MD5:	895004ddaa3758ac453d73e3d8c1f45f
SHA1:	0fb1a2c06513134ff699f4f286a71f1671918180
SHA256:	74ef237a5145c0d85ee7575c283493a2bd0ae116590c06749cf1ed72f655b997
SHA512:	af92b8bfe841b460373a9145dd30419f275751ee1edb2bf8c7af42629be6a48db7e0cc06abd10af3937a6e8a6b2b25994547541b4a21e65ea2398ba992f2aed9
SSDEEP:	768:L5UoJZS2vK+c+wdCAXNnZ98baBXe13jtCs8sNaHXsSsGtj+WNAMTauI:DZKCuCCZKt1z98scH8ucWBOP

TLSH:	0F43E155AE1D04FBC16781773735933AC2F7C22691182CCAC513AA6E6EBA613EC7D243
File Content Preview:	MZ.f.:.....@.....!..L.!This program cannot be run in DOS mode....$.....V...7...7...7.....7...O...7...7...7..;8...7..;8...7..;8...7.....7.....7.....7..Rich.7.....PE..L....T.b...

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10001d4b
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE, DLL
DLL Characteristics:	
Time Stamp:	0x629654C0 [Tue May 31 17:47:44 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	

Entrypoint Preview

Instruction
in al, dx
and ecx, 00000FFFh
add ecx, esi
add dword ptr [ecx], ebx
mov ebx, dword ptr [ebp-08h]
inc ebx
inc ebx
dec dword ptr [ebp-0Ch]
mov dword ptr [ebp-08h], ebx
jne 00007F377CCD8233h
mov ecx, dword ptr [edi+04h]
sub dword ptr [ebp-04h], ecx
add edi, ecx
cmp dword ptr [ebp-04h], 08h
jnbe 00007F377CCD81FEh
pop edi
pop esi
pop ebx
leave
retn 0004h
cmp dword ptr [esp+08h], 00000000h
je 00007F377CCD8288h
mov ecx, dword ptr [eax+0Ch]
mov edx, ecx
sub edx, dword ptr [esp+04h]
mov dl, byte ptr [edx]
mov byte ptr [ecx], dl

Instruction
inc dword ptr [eax+0Ch]
dec dword ptr [esp+08h]
jne 00007F377CCD825Ch
ret
push ebp
mov ebp, esp
sub esp, 30h
push ebx
push esi
push edi
mov esi, eax
xor eax, eax
lea edi, dword ptr [ebp-28h]
stosd
stosd
stosd
stosd
stosd
xor ebx, ebx
xor eax, eax
push ebx
push 08000000h
push dword ptr [esi+08h]
lea edi, dword ptr [ebp-10h]
stosd
mov eax, dword ptr [esi+04h]
mov dword ptr [ebp-14h], eax
lea eax, dword ptr [ebp-14h]
push eax
lea eax, dword ptr [ebp-2Ch]
push eax
push 000F001Fh
lea eax, dword ptr [ebp-0Ch]
push eax
mov dword ptr [ebp-0Ch], ebx
mov dword ptr [ebp-08h], ebx
mov dword ptr [ebp-2Ch], 00000018h
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-20h], 00000040h
mov dword ptr [ebp-24h], ebx
mov dword ptr [ebp-1Ch], ebx
mov dword ptr [ebp-18h], ebx
call dword ptr [esi+0Ch]
cmp eax, ebx
jl 00007F377CCD82A7h
mov eax, dword ptr [ebp-0Ch]
mov dword ptr [esi], eax
lea eax, dword ptr [ebp-08h]
push eax
call 00007F377CCD8D1Dh
mov edi, eax
cmp edi, ebx
jne 00007F377CCD828Bh
push dword ptr [ebp-14h]
push ebx

Rich Headers

Programming Language:	• [ASM] VS2005 build 50727 • [IMP] VS2008 SP1 build 30729 • [EXP] VS2005 build 50727 • [LNK] VS2005 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x35f0	0x4f	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x312c	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6000	0x154	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3000	0xcc	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1797	0x1800	False	0.3787434895833333	data	4.019765538082408	IMAGE_SCN_CNT_CODE, IMAGE_SCN_LNK_OVER, IMAGE_SCN_LNK_REMOVE, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_MEM_PRELOAD, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_128BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x3000	0x63f	0x800	False	0.7646484375	data	6.425623877611753	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_OVER, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_MEM_PURGEABLE, IMAGE_SCN_MEM_16BIT, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_128BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
.data	0x4000	0x24c	0x200	False	0.875	data	5.824857955609047	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_INFO, IMAGE_SCN_LNK_OVER, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_MEM_PRELOAD, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0x5000	0x26c	0x400	False	0.3603515625	data	3.17724172343837	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_OVER, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_MEM_SYSHEAP, IMAGE_SCN_MEM_PURGEABLE, IMAGE_SCN_MEM_16BIT, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

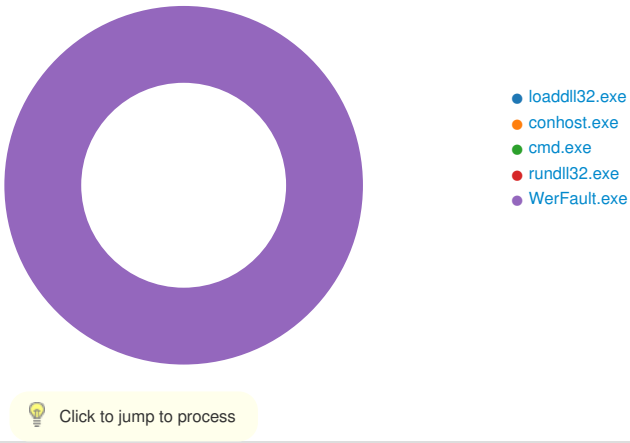
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x6000	0x8000	0x7200	False	0.5444078947368421	data	5.290169344471963	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_LNK_OVER, IMAGE_SCN_GPREL, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_128BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **5984**, Parent PID: **3528**

General

Target ID:	0
Start time:	20:02:27

Start date:	16/03/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\unpacked (1).dll"
Imagebase:	0x890000
File size:	116736 bytes
MD5 hash:	1F562FBF37040EC6C43C8D5EF619EA39
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5980, Parent PID: 5984

General

Target ID:	1
Start time:	20:02:27
Start date:	16/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6032, Parent PID: 5984

General

Target ID:	2
Start time:	20:02:27
Start date:	16/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\unpacked (1).dll",#1
Imagebase:	0xd90000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **6092**, Parent PID: **6032**

General

Target ID:	3
Start time:	20:02:27
Start date:	16/03/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\unpacked (1).dll",#1
Imagebase:	0x870000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: **1236**, Parent PID: **6092**

General

Target ID:	6
Start time:	20:02:28
Start date:	16/03/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6092 -s 636
Imagebase:	0x1310000
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	6CCE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9852.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9852.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CCD497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7bde5861e98b2ac3cc37e329f3101f62f0fff922_82810a17_049ebf60	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7bde5861e98b2ac3cc37e329f3101f62f0fff922_82810a17_049ebf60\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CCD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9852.tmp	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9852.tmp.xml	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER985F.tmp.csv	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER98FD.tmp.txt	success or wait	1	6CCD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 67 13 64 fd 05 12 00 00 00 00 00	MDMP gd	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	6976	6	00 00 00 00 00 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.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 40 1b 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 17 00 00 fd 67 13 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 01 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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	UB@GenuineIntelWTgd01W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	8186	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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 18 7b fd 02 01 00 00 00 00 00 00 00 0f fd fd fd 38 31 00 10 00 00 00 10 fd fd 77 00 3b 07 fd 77 23 00 00 00 02 02 01 00 fd fd 77 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 fd fd	+S++{81w;w#w+	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	1620	168	fd 17 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 3b 07 fd 77 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 1f 00 00	;w	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	10334	20	0c 00 00 00 fd 06 fd 77 00 00 00 00 00 01 00 00 22 29 00 00	w")	success or wait	12	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	10530	256	53 56 fd fd 57 fd 74 24 0c fd 46 10 00 00 fd 00 fd 46 20 fd 44 24 10 75 15 fd fd fd 25 fd 01 00 fd 09 5c 24 18 fd fd 0f fd fd 01 00 00 fd fd fd 42 fd 01 00 fd 09 44 24 18 fd fd 0f fd fd 01 00 00 fd 7e 3c 00 0f fd 74 01 00 00 fd fd fd fd 01 00 33 fd fd 44 24 24 fd 78 0c fd 7c 24 20 39 37 0f fd fd 01 00 00 fd fd 33 cb 7c 24 10 fd 64 24 00 fd 51 04 fd fd 74 13 fd 47 18 46 fd 3c 02 00 74 01 43 fd fd 14 fd 39 00 75 fd 7c 24 20 fd c9 5c 24 14 fd 5c 24 18 0f fd 5c 01 00 00 fd 0d fd 7b fd 77 fd 04 fd 00 00 00 00 fd fd 00 00 18 00 50 fd fd 08 51 fd 35 fd 7b fd 77 fd 3e 00 00 fd 4c 24 0c fd 41 30 fd fd 0f fd fb 04 00 fd 44 24 24 fd 71 34 fd fd fd 44 24 1c 00 00 00 00 fd 46 4c fd 44 24 14 40 fd 46 38 fd 3f 00 0f fd fd 00 00 00 fd 54 24 10 33	SVWt$FF D$u%\$BD$~ <t3D$$x\|$ 97 3\|dQtGF<tC9u\|$ \$\$\ {wPQ5{w> L$A0D$$q4DFLD@F8 ?T$3	success or wait	11	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	25810	4096	fd fd fd 02 00 00 fd 02 00 40 fd 02 00 00 00 00 00 1e 00 00 00 00 00 00 00 60 fd 02 00 00 00 00 fd 17 00 00 fd 17 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 77 09 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	@`pw	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	8902	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 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 fd fd fd fd 38 31 00 10 00 00 00 00 fd fd 77 00 fd fd fd 77 23 00 00 00 12 02 00 00 10 fd 77 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++81ww#w+	success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	1840	48	fd 17 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 60 fd 02 00 00 00 00 fd fd fd 02 00 00 00 00 14 08 00 00 16 46 00 00 fd 02 00 00 fd 25 00 00	`F%	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	1900	4	29 00 00 00	)	success or wait	41	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	6982	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	41	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	6224	752	00 00 00 10 00 00 00 00 00 fd 00 00 00 00 00 00 fd 54 fd 62 fd 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 36 7a 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 7b 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 4d 6f 1b 00 00 00 00 00 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 04 00 00 00 00	TbZb6z{Mo@	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	29906	9296	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 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 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	EventFileFile(WaitCompletionPa cketIoCompletionTpWorkerFactor yIRTimer(WaitCompletion PacketIRTim	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER962D.tmp.dmp	32	108	03 00 00 00 64 00 00 00 fd 06 00 00 04 00 00 00 50 11 00 00 6c 07 00 00 05 00 00 00 fd 00 00 00 5e 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 60 19 00 00 fd 7f 00 00 15 00 00 00 fd 01 00 00 fd 18 00 00 16 00 00 00 fd 00 00 00 fd 1a 00 00	dPl^(T8T`	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 30 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6092</Pid>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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 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>000000000</CmdLineSignature>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 39 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2095</Uptime>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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 31 00 39 00 39 00 35 00 39 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>119959552</PeakVirtualSize>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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 31 00 39 00 36 00 32 00 33 00 36 00 38 00 30 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>119623680</VirtualSize>	success or wait	1	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.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 32 00 31 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>2165</PageFaultCount>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1696	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 37 00 32 00 30 00 30 00 37 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>7200768</PeakWorkingSetSize>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 32 00 30 00 30 00 37 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>7200768</WorkingSetSize>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 32 00 31 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 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>172128</QuotaPeakPagedPoolUsage>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 30 00 38 00 36 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>170864</QuotaPagedPoolUsage>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 30 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>22040</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21768</QuotaNonPagedPoolUsage>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2376	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 34 00 39 00 31 00 39 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>4919296</PagefileUsage>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2462	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 34 00 39 00 32 00 37 00 34 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>4927488</PeakPagefileUsage>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2564	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 34 00 39 00 31 00 39 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>4919296</PrivateUsage>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2644	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2698	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2738	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 30 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6032</Pid>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2832	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 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>cmd.exe</ImageName>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2904	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000 00000</Cm dLineSignature>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3006	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 31 00 36 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2167</Uptime>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3060	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3154	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3218	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	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3276	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 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 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>57405440</PeakVirtualSize>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3376	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 35 00 33 00 34 00 34 00 30 00 35 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>53440512</VirtualSize>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3460	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 31 00 31 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>1112</PageFaultCount>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3548	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 33 00 36 00 38 00 36 00 34 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3686400</PeakWorkingSetSize>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3658	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 33 00 36 00 37 00 34 00 31 00 31 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>3674112</WorkingSetSize>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3752	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 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 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>40960</QuotaPeakPagedPoolUsage>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3878	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>33216</QuotaPagedPoolUsage>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	3988	122	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 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5632</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4124	106	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 32 00 32 00 34 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>5224</QuotaNonPagedPoolUsage>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4244	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 33 00 36 00 35 00 34 00 34 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>3436544</PagefileUsage>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4334	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 33 00 35 00 38 00 38 00 30 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3588096</PeakPagefileUsage>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4440	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 33 00 36 00 35 00 34 00 34 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>3436544</PrivateUsage>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4524	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4580	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4630	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4668	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4716	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4762	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	4832	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	5442	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	5446	2	09 00		success or wait	1	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	5448	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	5488	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	5492	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	5494	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	6	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	12	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	5540	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6094	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6098	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6100	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6140	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6144	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6146	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6192	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	2	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6294	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 69 00 6b 00 79 00 61 00 71 00 65 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>ikyaqe, Inc.</SystemManufacturer>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6400	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6404	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6408	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 69 00 6b 00 79 00 61 00 71 00 65 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>ikyaqe7,1</SystemProductName>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6504	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6508	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6512	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6640	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 33 00 38 00 32 00 39 00 37 00 38 00 33 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>1638297834</OSInstallDate>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6722	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6726	2	09 00		success or wait	2	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6730	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6840	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6910	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6914	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6916	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6956	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6960	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6962	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7004	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7106	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	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7142	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7146	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7148	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	3	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	6	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7180	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 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7424	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7428	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7430	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7456	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7460	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7462	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 33 00 2d 00 31 00 36 00 54 00 31 00 39 00 3a 00 30 00 32 00 3a 00 32 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-03-16T19:02:29Z">	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	2	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7570	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 32 00 39 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 30 00 39 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 31 00 35 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 35 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="297" PID="6092" UptimeMS="156" TimeSinceCreationMS="156" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7828	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7832	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7836	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7856	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7860	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7862	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7900	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7904	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7906	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	7952	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 37 00 65 00 37 00 38 00 61 00 31 00 35 00 2d 00 36 00 39 00 34 00 65 00 2d 00 34 00 63 00 38 00 35 00 2d 00 62 00 65 00 30 00 36 00 2d 00 62 00 35 00 34 00 31 00 33 00 33 00 31 00 33 00 30 00 30 00 31 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>27e78a15-694e-4c85-be06-b54133130014</Guid>	success or wait	1	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	8050	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	8054	2	09 00		success or wait	2	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	8058	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 33 00 2d 00 31 00 36 00 54 00 31 00 39 00 3a 00 30 00 32 00 3a 00 32 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-03-16T19:02 :29Z</CreationTime>	success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	8156	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	8160	2	09 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	8162	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	8202	4	0d 00 0a 00		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97E3.tmp.WERInternalMetadata.xml	8206	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9852.tmp.xml	0	4630	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	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7bde5861e98b2ac3cc37e329f3101f62f0fff922_82810a17_049ebf60\Report.wer	0	2	fd fd		success or wait	1	6CCD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7bde5861e98b2ac3cc37e329f3101f62f0fff922_82810a17_049ebf60\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	167	6CCD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7bde5861e98b2ac3cc37e329f3101f62f0fff922_82810a17_049ebf60\Report.wer	11046	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 37 00 31 00 37 00 33 00 35 00 37 00 31 00 35 00 32 00	MetadataHash=717357152	success or wait	1	6CCD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6CCF36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6CCF1FB2	RegCreateKeyExW
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CCD43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LongPathHash	unicode	rundll32.exe\ab97b57a	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6CCF36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6CCF36BF	unknown
\REGISTRY\A\{df7da023-c581-cc97-75cf-8a23aca8c356}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6CCF36BF	unknown
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 3B 07 D4 77 02 00 00 00 00 00 00 00 0F 92 C2 E1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6CCF1FE8	RegSetValueExW

Disassembly

No disassembly