ID: 564921
Sample Name: knigger.dll
Cookbook: default.jbs
Time: 15:51:13
Date: 02/02/2022
Version: 34.0.0 Boulder Opal

Table of Contents

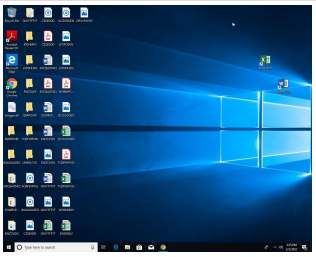
Windows Analysis Report

knigger.dll

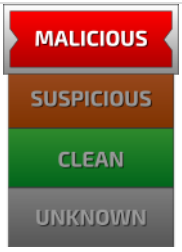
Overview

General Information

Sample Name:	knigger.dll
Analysis ID:	564921
MD5:	f2fdb0f416abda7..
SHA1:	cb35382ae44bc4..
SHA256:	5e5242e1251bfb..
Infos:	



Detection



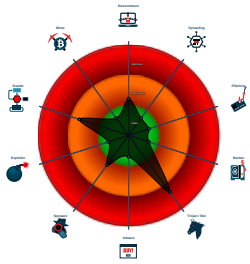
Dridex

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: Suspicious Call by…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- AV process strings found (often use…
- Yara signature match
- Sample file is different than original …
- One or more processes crash

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4828 cmdline: loaddll32.exe "C:\Users\user\Desktop\knigger.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 160 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\knigger.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 2964 cmdline: rundll32.exe "C:\Users\user\Desktop\knigger.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 4628 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2964 -s 696 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 22201,
  "C2 list": [
    "144.91.122.100:443",
    "188.214.241.242:4664",
    "93.104.209.107:8116",
    "5.189.190.214:593"
  ],
  "RC4 keys": [
    "S9OYlNFUvY5N1RDSpi8BgH6SgS8gPIcU",
    "rRgzULsP0KBJ7CcLRdZ7mhoBdNxJNQSrQLI3uRuRJVi7lqosB75laFDkwhMJ8LECg1b8sYjJZr"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.368054166.0000000002D40000.00000040.00000800.00020000.00000000.sdmp	MALWARE_Win_DLLLoader	Detects unknown DLL Loader	ditekSHen	• 0x3063:$s1: LondLibruryA • 0x304e:$s2: LdrLoadDll • 0x3059:$s3: snxhk.dll • 0x30f6:$s4: DisableThreadLibraryCalls
00000003.00000002.368122087.000000006ED81000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.454c63b.1.unpack	MALWARE_Win_DLLLoader	Detects unknown DLL Loader	ditekSHen	• 0xcf3:$s1: LondLibruryA • 0xcde:$s2: LdrLoadDll • 0xce9:$s3: snxhk.dll • 0xd86:$s4: DisableThreadLibraryCalls
3.2.rundll32.exe.2d40000.0.unpack	MALWARE_Win_DLLLoader	Detects unknown DLL Loader	ditekSHen	• 0x1a93:$s1: LondLibruryA • 0x1a7e:$s2: LdrLoadDll • 0x1a89:$s3: snxhk.dll • 0x1b26:$s4: DisableThreadLibraryCalls
3.2.rundll32.exe.454c63b.1.raw.unpack	MALWARE_Win_DLLLoader	Detects unknown DLL Loader	ditekSHen	• 0x1a93:$s1: LondLibruryA • 0x1a7e:$s2: LdrLoadDll • 0x1a89:$s3: snxhk.dll • 0x1b26:$s4: DisableThreadLibraryCalls
3.2.rundll32.exe.2d40000.0.raw.unpack	MALWARE_Win_DLLLoader	Detects unknown DLL Loader	ditekSHen	• 0x3063:$s1: LondLibruryA • 0x304e:$s2: LdrLoadDll • 0x3059:$s3: snxhk.dll • 0x30f6:$s4: DisableThreadLibraryCalls
3.2.rundll32.exe.6ed80000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Sigma Overview

System Summary

Sigma detected: Suspicious Call by Ordinal

Jbx Signature Overview

AV Detection

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Dridex unpacked file

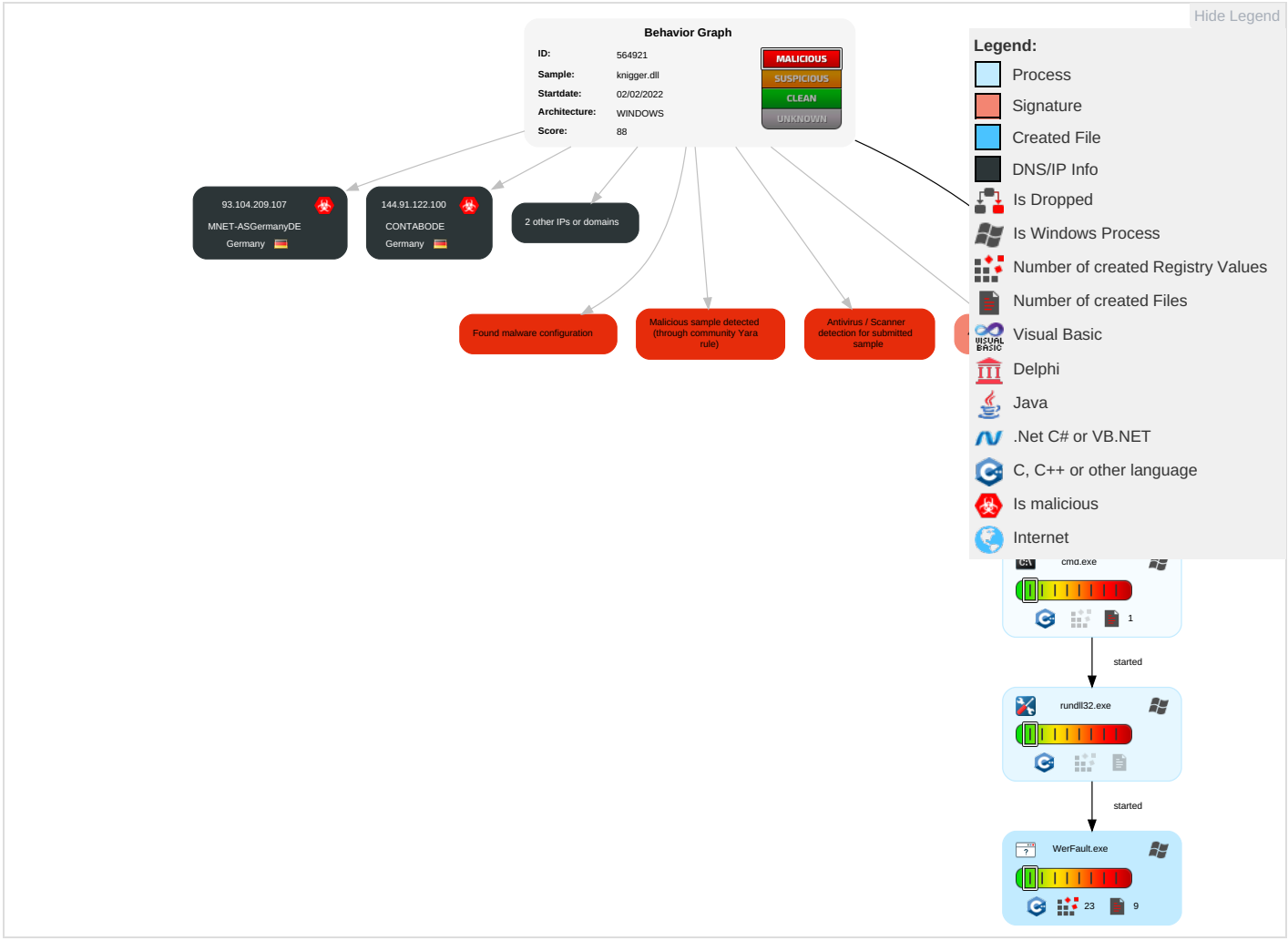
System Summary

Malicious sample detected (through community Yara rule)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Disable or Modify Tools	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	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 Virtualization/Sandbox Evasion	LSASS Memory	3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	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 1 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	1 Account 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 Rundll32	LSA Secrets	1 System Owner/User Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 1 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

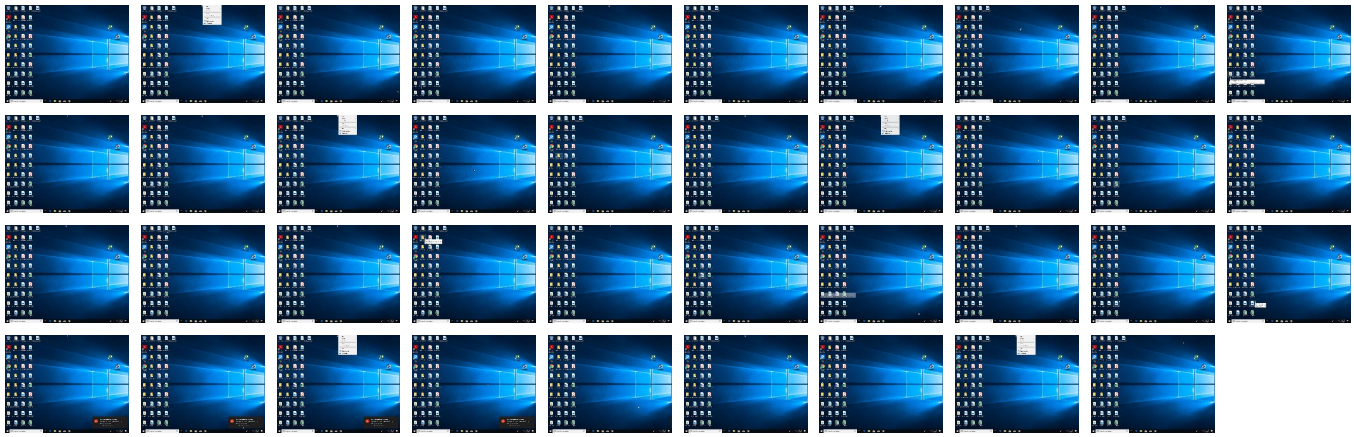
Behavior Graph



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
knigger.dll	59%	Virustotal		Browse
knigger.dll	70%	ReversingLabs	Win32.Trojan.Drixed	
knigger.dll	100%	Avira	TR/Crypt.Agent.pvvzj	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.6ed80000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.2.rundll32.exe.2d40000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.kazanfirst.ruDVarFileInfo$	0%	Avira URL Cloud	safe	

Domains and IPs

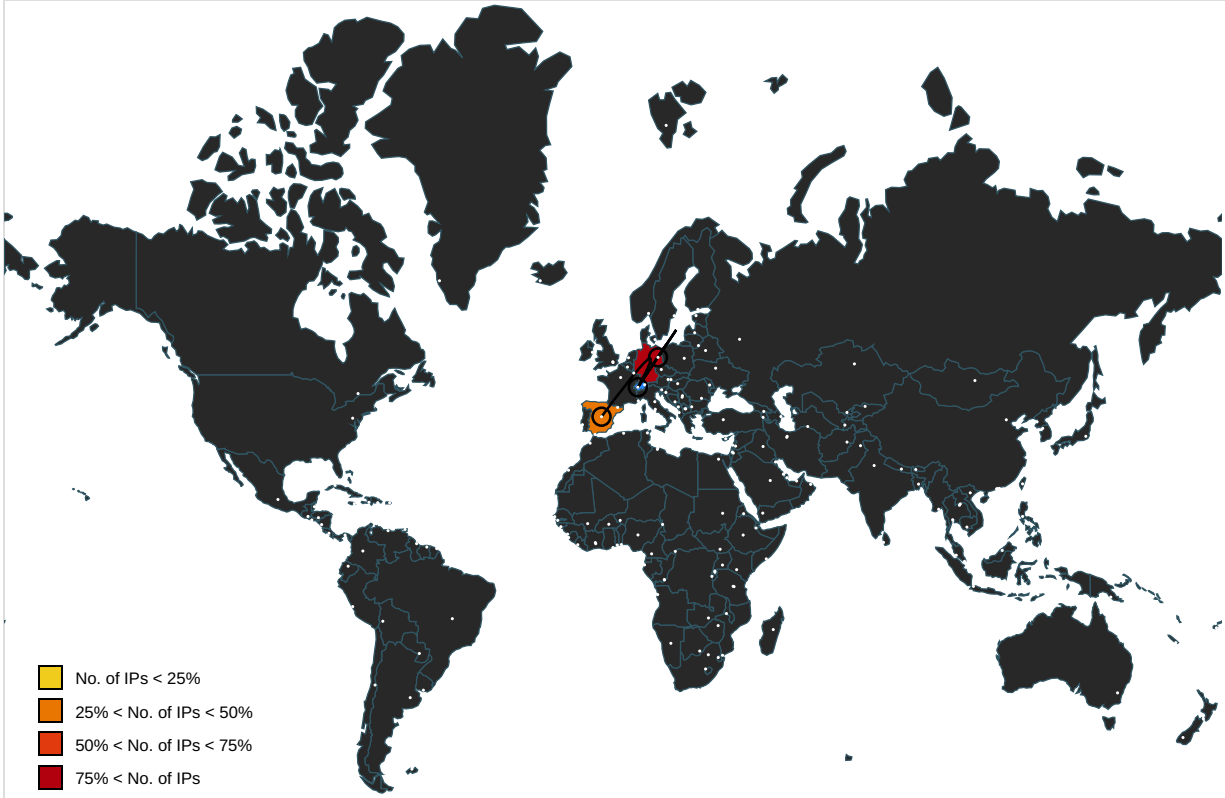
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://upx.sf.net	Amcache.hve.12.dr	false		high
http://www.kazanfirst.ruDVarFileInfo$	rundll32.exe, 00000003.00000002.36825143 0.000000006ED9F000.00000002.00000001.010 00000.00000003.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.214.241.242	unknown	Spain		62412	BORECOM-INNOVABorecom-InnovaES	true
93.104.209.107	unknown	Germany		8767	MNET-ASGermanyDE	true
144.91.122.100	unknown	Germany		51167	CONTABODE	true
5.189.190.214	unknown	Germany		51167	CONTABODE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	564921

Start date:	02.02.2022
Start time:	15:51:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	knigger.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.troj.winDLL@8/6@0/4
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 95.6% (good quality ratio 93.7%) • Quality average: 78.9% • Quality standard deviation: 25.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.60.218.8, 2.18.100.248, 20.42.65.92
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, e11290.dspg.akamaiedge.net, e13551.dscg.akamaiedge.net, msagfx.live.com-6.edgekey.net, authgfx.msa.akadns6.net, go.microsoft.com, onedsblobprdeus17.eastus.cloudapp.azure.com, store-images.s-microsoft.com, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, clientconfig.passport.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_88c9a135c9b22294e84c86e44fa262283b2da9a_82810a17_12540027\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9319943565912974
Encrypted:	false
SSDEEP:	192:Xqqi4r0oXbHBUZMX4jed+v/u7sUS274ItWc:6qiyX7BUZMX4je6/u7sUX4ItWc
MD5:	A3176A8BDEA8FB06C0B6B4CBC289CAB9
SHA1:	9C0FBA53F61D7A2C44A1B48EA028796FFBF11A0B
SHA-256:	90E5FFB56BF17914BA4E88D12F7EA56E618615BE4E10D628E2D504A4F85323AB
SHA-512:	74A86F7EEDD3ECC259AABA4B3C62CBF346F86D0047E5802DE30BE499E995E17344DD7C5C304A4F0188611864C7540DA50A19F14B899519C246442B732F9E567
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.=.1.3.2.8.8.3.1.9.5.5.4.5.3.3.4.9.6.6.....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.=.1.3.2.8.8.3.1.9.5.8.6.8.9.2.7.9.2.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.a.8.6.4.d.1.9.-.9.f.b.e.-.4.a.4.c.-.9.9.a.4.-.4.9.7.5.7.0.5.e.f.d.8.5.....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.=.4.3.4.a.3.2.1.5.-.5.3.3.2.-.4.9.5.1.-.b.8.c.b.-.b.e.a.4.2.3.3.8.6.9.0.7.....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.=.0.0.0.0.0.b.9.4.-.0.0.0.1.-.0.0.1.6.-.7.8.1.9.-.2.0.e.8.8.f.1.8.d.8.0.1.....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\WER79C1.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 2 23:52:35 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	48164
Entropy (8bit):	2.2817264569038596
Encrypted:	false
SSDEEP:	192:pgGiuhOUfSjSaO5Skb0HYvkED4YFRFwmYmxOC09j7MU0ZoYnbk:/oUfN5LbSmkEDXwmYmUC09PHGTQ
MD5:	E4717D87C6878FA123DAA111649FCE14
SHA1:	BB67AAB4CC9538260784238048152EA8915E6385
SHA-256:	C4DE107F24C62DBD7FD78CA7A90D27CA64C0353255942A6069FAB25D8715336C
SHA-512:	F0FEE9945D4BF5A0B1E0B5749EC3DF4E1D3B617B0E1BE37F220BC72C4B7A7E4AC8F27C4138BB0874AA975B4A5102F9BB2801147BA44FF449473413AEAAD5E687
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....C..a.....D.....T.....8.....T.....U.....B.....d.....GenuineIntelW.....T.....0..a.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe

File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8248
Entropy (8bit):	3.691363996739297
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNic46Pn6YkG63gmfTTSsCprR89bj9sftcBm:RrlsNib6v6Yt63gmfTTSKj2ft3
MD5:	CAE74CD0A1C22C113376403DCA715008
SHA1:	30ED2770112BE253F736D5D08ADE7E0B0F3DC514
SHA-256:	F7A96B2CE4CC86DF7957A1DB405DBD857653BC8CB24FD8FB8CB1F516433031B2
SHA-512:	40975CC19844B7F578B9E16D2C77316E00FCEDE707E57503CE192196B18BEEFEE1EA7B3A46B5E2E810B42CF39522572F3702531C6164ABF3614276E6EC78EE1
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.>.2.9.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8135.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4624
Entropy (8bit):	4.454457460508943
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6+JgtWI9LqkWSC8Be/8fm8M4JCdsL2jGFj+q8/iKYRXm4SrSXd:uITfVQqSNZJJv34DWXd
MD5:	27D6E50B5EB6AEF6A2D54A856E51E968
SHA1:	9DD8CA00D30110A23CF9484F0A4090D73C43EDDE
SHA-256:	6C493A35648E9AF30EC079CF9A70453D68E81E52D6913F7C85FC2862967EAD25
SHA-512:	8E26C0A4656B66AEB612FF99BCB9F71B6C8163CA4188D4B9C036A82E084DB255E339EBC082DE3E61A650C78707B9CB5DCDE7656F161A71196D64D2BBBD4E1DDF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1369983" />.. <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):	4.267411324011277
Encrypted:	false
SSDEEP:	12288:Nc03wPd7i7/6cxhKWe0OdaTZmLpmM9hRojfdDRQw32UFAnB0N5DH5mBp:e03wPd7i7/6cxhKdUINp
MD5:	F4E60B2B504C8CA455D53506B2AE7B26
SHA1:	9927BFEEA9D5239DF52AAC89A8E44AF04D9D455B
SHA-256:	192E18F0E00215426850CB7306BE8DDC6CE497677AC902A151754BF8EC4B9DF0
SHA-512:	91B882D9978C5729E2379F7591F8A740DE0526DF73B91D505DBBD4DE6C692524EFC5EF3006E1D85D43FDD5CC6938659732BA4D4E9EB30029E77BF34230BB7CB
Malicious:	false
Reputation:	low
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.rmtmn..... ....

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):	3.8392122514635516
Encrypted:	false
SSDEEP:	384:y0q5WZrdwdXX5QQp8XXLnxOf2ozPmxwpS5GjZmGu8DTTeC5N5PAR1K:l0UrmXXxpigf2oSxwpuWmGuSTemN5oR1
MD5:	52A7489E65BF4ED3609EBDAFAB21045D
SHA1:	6BB634FE807186A287A5D3F084F72EDC59A42DFB
SHA-256:	4DFB7F4BB140175A928958F47867C297FE9B6D9E6D83674E6D46AF3E5DE90A28
SHA-512:	31650AFA27AF5978A7CE1E79DCA41BE7D1971E795FE068AFB2A53FE483F5159D5903E5D60F45A1FE467029771E2BF501254B3E09B2DF94B3808749D1F00C019F
Malicious:	false
Reputation:	low
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.rmtmn..... ....HvLE.^.....P.....e...4$*.P.r..... ..hbin.....p.\..,.....nk,..`.....H..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..`..... .....P..... .....Z.....Root.....lf.....Root....nk ..`.....}..... .....*.....DeviceCensus..... ....vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.311800540085467
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:	knigger.dll
File size:	520192
MD5:	f2fdb0f416abda7c5fb8436578f1b6c8
SHA1:	cb35382ae44bc43c1372a21b04fc214885a4d8f2
SHA256:	5e5242e1251bfb745e068b413dab59a74afe94850e1b8d02acb607c50ce63fd0
SHA512:	e0a5bb0fbcb0732f4dc1450de7d7a75a47408233e2ee669d574788ea0e87ca39ba4ae4aa7a93d4bbaa73a7042eb0ab147348243397a3418af09ce14e347dcfda
SSDEEP:	6144:55a3RjZ1XrZvR7Z9JrZdR5ZbR1Z9RVZ1RvZpR17fRrZpRrTZRfZ3Rr3fRJZfRlZ3:obTFRJXfZrFTfVBokoa7fGs8k7l
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R...<...<...<..k....<...=.S.<.=.....<.....<.....<.t.?...<.t.=.4.<.L.9...<.t..0.<..k....<..0..x.<.....<..1....<..k....<

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10005000
Entrypoint Section:	.rdata
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61C045E9 [Mon Dec 20 08:59:21 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0

Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	2b1b4edc6ebe7eca63696f6220126258

Entrypoint Preview
Instruction
mov edx, 00000003h
cmpps xmm1, xmm0, 02h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
add edx, 04h
call 00007F5464A7BFD2h
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push ebx
push edi
push esi
and esp, FFFFFFF8h
sub esp, 00000088h
mov eax, dword ptr [ebp+08h]
mov byte ptr [esp+77h], 00000018h
mov ecx, dword ptr [esp+78h]
mov edx, dword ptr [esp+7Ch]
mov esi, ecx
or esi, 37041D98h
mov dword ptr [esp+78h], esi
mov bl, byte ptr [esp+77h]

Instruction
mov bh, bl
xor bh, FFFFFFCDh
mov byte ptr [esp+4Fh], bh
mov dword ptr [esp+34h], eax
mov dword ptr [esp+30h], ecx
mov dword ptr [esp+2Ch], edx
mov byte ptr [esp+2Bh], bl
call 00007F5464A7F9C8h
xor ecx, ecx
mov di, word ptr [esp+6Ch]
mov word ptr [esp+6Ch], di
mov edx, eax
mov esi, dword ptr [eax+3Ch]
mov bl, byte ptr [esp+2Bh]
xor bl, 00000069h
mov dword ptr [esp+00h], eax

Rich Headers

Programming Language:	• [IMP] VS2015 UPD1 build 23506 • [C++] VS2012 UPD1 build 51106 • [ASM] VS2012 build 50727 • [ASM] VS2012 UPD2 build 60315 • [LNK] VS2010 SP1 build 40219 • [EXP] VS2010 SP1 build 40219 • [RES] VS2015 UPD1 build 23506 • [IMP] VS2010 build 30319 • [ASM] VS2015 UPD1 build 23506 • [C++] VS2017 v15.5.4 build 25834 • [EXP] VS2012 UPD4 build 61030 • [C++] VS2008 build 21022 • [ASM] VS2010 SP1 build 40219

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x76d43	0x60	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x76e1c	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7f000	0x2f0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x80000	0x8d8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x6030	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x54	.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
.rdata	0x1000	0x69ae	0x7000	False	0.381487165179	data	4.43403192783	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x6f052	0x70000	False	0.29494367327	data	7.44583798287	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x78000	0x6428	0x5000	False	0.345947265625	data	5.9113186779	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x7f000	0x2f0	0x1000	False	0.09033203125	data	0.793575928673	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x80000	0x8d8	0x1000	False	0.275390625	data	4.1888764152	IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x7f060	0x290	MS Windows COFF PA-RISC object file	English	United States

Imports

DLL	Import
OPENGL32.dll	glTexImage2D
KERNEL32.dll	GetFileSize, GetModuleFileNameW, OutputDebugStringA, CloseHandle, IsDebuggerPresent, GetModuleHandleW
ADVAPI32.dll	QueryServiceStatusEx, RegCloseKey, AccessCheck
WINSPOOL.DRV	EnumFormsW
USER32.dll	GetWindowTextA
ole32.dll	PropVariantClear
WS2_32.dll	WSACleanup

Version Infos

Description	Data
OriginalFilename	Nrt.dll
FileDescription	Oracle Call Interface
FileVersion	9.6.7.6.0
Legal Copyright	Copyright Oracle Corporation 1979, 2001. All rights reserved.
CompanyName	Oracle Corporation
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **4828**, Parent PID: **5432**

General	
Target ID:	1
Start time:	15:52:15
Start date:	02/02/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\knigger.dll"
Imagebase:	0x850000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
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: cmd.exe PID: **160**, Parent PID: **4828**

General	
Target ID:	2
Start time:	15:52:15
Start date:	02/02/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\knigger.dll",#1
Imagebase:	0x150000
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: **2964**, Parent PID: **160**

General

Target ID:	3
Start time:	15:52:16
Start date:	02/02/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\knigger.dll",#1
Imagebase:	0x1e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: MALWARE_Win_DLLLoader, Description: Detects unknown DLL Loader, Source: 00000003.00000002.368054166.0000000002D40000.00000040.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.368122087.000000006ED81000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: **4628**, Parent PID: **2964**

General

Target ID:	12
Start time:	15:52:33
Start date:	02/02/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2964 -s 696
Imagebase:	0x11d0000
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	6E9E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E9D497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8135.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8135.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_88c9a135c9b22294e84c86e44fa262283b2da9a_82810a17_12540027	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_88c9a135c9b22294e84c86e44fa262283b2da9a_82810a17_12540027\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E9D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8135.tmp	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8135.tmp.xml	success or wait	1	6E9D497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 43 19 fd 61 fd 05 12 00 00 00 00 00	MDMP Ca	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	7780	6	00 00 00 00 00 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 64 1e 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 0b 00 00 30 19 fd 61 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 3d 00 00 00 00 00 00 00 01 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBdGenuineIntelWT0a0=Pacific Standard TimePacific Daylight Time	success or wait	1	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	9162	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 fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 04 01 00 00 28 fd fd 6e fd 06 fd 77 20 46 fd 77 fd 02 00 00 20 46 fd 77 00 00 00 00 52 36 fd 6e 23 00 00 00 02 02 00 00 fd fd 7a 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++(nw Fw FwR6n#z+	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	1620	168	14 14 00 00 00 00 00 00 03 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 52 36 fd 6e 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 23 00 00	R6n#	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	12026	20	0f 00 00 00 fd fd 7a 02 00 00 00 00 6c 1d 00 00 fd 2f 00 00	zl/	success or wait	15	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	12270	7532	fd fd fd 77 fd 1a 32 77 fd fd fd fd fd fd 7a 02 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 02 00 00 fd 02 00 00 fd fd fd fd 24 00 00 00 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 fd fd fd fd 00 30 fd 02 fd fd fd fd fd fd fd 00 00 00 00 fd fd 7a 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	w2wz$0z	success or wait	14	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	36266	1804	fd fd fd 77 fd 60 77 64 02 00 00 fd fd fd fd 10 00 00 00 fd fd fd 02 54 fd fd 02 fd fd fd fd 40 e0 77 40 e0 77 fd fd fd fd 00 fd fd 02 00 fd fd 02 00 00 00 00 64 02 00 00 fd fd fd fd 64 02 00 00 fd fd fd fd 00 fd fd 02 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 28 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 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 48 fd 02 00 00 00 00 00 00 00 00 00 60 fd 02 00 30 fd 02 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd 28 fd fd 02 54 32 fd 02 30 fd fd 02 58 fd 02 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwdT@w@wdd(H`0(T20X	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	9878	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 20 46 fd 77 fd fd fd fd 00 00 00 00 28 fd 7a 02 fd fd fd 77 23 00 00 00 02 02 00 00 fd fd 7a 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++ Fw(zw#z+	success or wait	3	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	1888	48	fd 07 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 02 00 00 00 00 5c fd fd 02 00 00 00 00 fd 08 00 00 5a 4e 00 00 fd 02 00 00 2e 2c 00 00	\ZN.,	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	1948	4	30 00 00 00	0	success or wait	48	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	7786	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	48	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	7028	752	00 00 05 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 23 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fd 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 00 70 fd 02 00 00 00 00 28 2d 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 62 03 00 00 00 00 00 fd 62 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 5f 1b 00 00 00 00 00 22 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 79 fd 04 00 00 00 00	t0Us@#BB?#@AZbp(-bb_"@y	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	38070	10094	12 00 00 00 44 00 69 00 72 00 65 00 63 00 74 00 6f 00 72 00 79 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 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61	DirectoryFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPa	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79C1.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 44 14 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 2e 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 08 1c 00 00 1c fd 00 00 15 00 00 00 fd 01 00 00 fd 1b 00 00 16 00 00 00 fd 00 00 00 fd 1d 00 00	D.T8T	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 32 00 39 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>2964</Pid>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 38 00 31 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>19815</Uptime>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1230	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1320	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1380	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1434	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 32 00 38 00 34 00 37 00 31 00 30 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>128471040</PeakVirtualSize>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1532	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 32 00 37 00 30 00 39 00 38 00 38 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>127098880</VirtualSize>	success or wait	1	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1604	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1608	2	09 00		success or wait	3	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1614	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 37 00 39 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2799</PageFaultCount>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1688	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1692	2	09 00		success or wait	3	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1698	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 39 00 36 00 33 00 33 00 37 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>9633792</PeakWorkingSetSize>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1794	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1798	2	09 00		success or wait	3	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1804	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 39 00 36 00 33 00 33 00 37 00 39 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>9633792</WorkingSetSize>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1884	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1888	2	09 00		success or wait	3	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	1894	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 32 00 37 00 33 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	<QuotaPeakPagedPoolUsage>182736</QuotaPeakPagedPoolUsage>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2008	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2012	2	09 00		success or wait	3	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2018	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 32 00 34 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>182472</QuotaPagedPoolUsage>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2116	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2120	2	09 00		success or wait	3	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2126	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 37 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>15752</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2250	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2254	2	09 00		success or wait	3	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2260	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 33 00 35 00 30 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>13504</QuotaNonPagedPoolUsage>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2368	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2372	2	09 00		success or wait	3	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2378	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 36 00 35 00 30 00 30 00 33 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>6500352</PagefileUsage>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2454	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2458	2	09 00		success or wait	3	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2464	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 36 00 35 00 30 00 34 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>6504448</PeakPagefileUsage>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2556	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2560	2	09 00		success or wait	3	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2566	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 36 00 35 00 30 00 30 00 33 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>6500352</PrivateUsage>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2638	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2642	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2646	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2692	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2696	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2700	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2730	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2734	2	09 00		success or wait	3	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2740	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2780	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2784	2	09 00		success or wait	4	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2792	28	3c 00 50 00 69 00 64 00 3e 00 31 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>160</Pid>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.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 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3006	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 34 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>20246</Uptime>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3050	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3054	2	09 00		success or wait	4	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3062	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3144	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3148	2	09 00		success or wait	4	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3156	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3208	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3212	2	09 00		success or wait	4	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3220	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	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3264	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3268	2	09 00		success or wait	5	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3278	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3364	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3368	2	09 00		success or wait	5	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3378	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3448	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3452	2	09 00		success or wait	5	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3462	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 32 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>1122</PageFaultCount>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3536	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3540	2	09 00		success or wait	5	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3550	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 37 00 30 00 36 00 38 00 38 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>3706880</PeakWorkingSetSize>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3646	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3650	2	09 00		success or wait	5	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3660	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 39 00 34 00 35 00 39 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>3694592</WorkingSetSize>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3740	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3744	2	09 00		success or wait	5	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3754	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3866	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3870	2	09 00		success or wait	5	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3880	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3976	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3980	2	09 00		success or wait	5	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	3990	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4112	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4116	2	09 00		success or wait	5	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4126	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4232	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4236	2	09 00		success or wait	5	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4246	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 32 00 34 00 32 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3424256</PagefileUsage>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4322	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4326	2	09 00		success or wait	5	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4336	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 37 00 35 00 38 00 30 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>3575808</PeakPagefileUsage>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4428	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4432	2	09 00		success or wait	5	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4442	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 32 00 34 00 32 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3424256</PrivateUsage>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4514	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4518	2	09 00		success or wait	4	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4526	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4572	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4576	2	09 00		success or wait	3	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4582	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4624	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4628	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4632	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4670	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4712	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4716	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4718	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4764	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4826	4	0d 00 0a 00		success or wait	8	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4830	2	09 00		success or wait	16	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	4834	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	5438	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	5442	2	09 00		success or wait	1	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	5444	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	5484	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	5488	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	5490	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	5528	4	0d 00 0a 00		success or wait	6	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	5532	2	09 00		success or wait	12	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	5536	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6090	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6094	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6096	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6136	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6140	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6142	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6180	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6184	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6188	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6282	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6286	2	09 00		success or wait	2	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6290	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 6b 00 73 00 6e 00 63 00 68 00 71 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>ksnchq, Inc.</SystemManufacturer>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6396	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6400	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6404	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 6b 00 73 00 6e 00 63 00 68 00 71 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>ksnchq7,1</SystemProductName>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6500	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6504	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6508	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 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 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.13989454.B64.1906190538</BIOSVersion>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6628	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6632	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6636	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 35 00 38 00 33 00 34 00 38 00 38 00 38 00 36 00 32 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1583488622</OSInstallDate>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6718	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6722	2	09 00		success or wait	2	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6726	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6828	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6832	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6836	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6910	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6950	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6954	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6956	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	6998	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7100	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	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7136	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7140	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7142	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7166	4	0d 00 0a 00		success or wait	3	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7170	2	09 00		success or wait	6	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7174	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7422	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7426	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7428	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7454	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7458	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7460	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 32 00 2d 00 30 00 32 00 54 00 32 00 33 00 3a 00 35 00 32 00 3a 00 33 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-02-02T23:52:36Z">	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7560	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7564	2	09 00		success or wait	2	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7568	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 37 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 39 00 36 00 34 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 32 00 34 00 39 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 32 00 34 00 39 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	<Process AsId="370" PID="2964" UptimeMS="1249" TimeSinceCreationMS="1249" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7830	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7834	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7838	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7858	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7862	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7864	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7902	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7906	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7908	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7946	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7950	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	7954	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 61 00 38 00 36 00 34 00 64 00 31 00 39 00 2d 00 39 00 66 00 62 00 65 00 2d 00 34 00 61 00 34 00 63 00 2d 00 39 00 39 00 61 00 34 00 2d 00 34 00 39 00 37 00 35 00 37 00 30 00 35 00 65 00 66 00 64 00 38 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>0a864d19-9fbe-4a4c-99a4-4975705efd85</Guid>	success or wait	1	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	8052	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	8056	2	09 00		success or wait	2	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	8060	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 32 00 2d 00 30 00 32 00 54 00 32 00 33 00 3a 00 35 00 32 00 3a 00 33 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-02-02T23:52:36Z</CreationTime>	success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	8158	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	8162	2	09 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	8164	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	8204	4	0d 00 0a 00		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F40.tmp.WERInternalMetadata.xml	8208	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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8135.tmp.xml	0	4624	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 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	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_88c9a135c9b22294e84c86e44fa262283b2da9a_82810a17_12540027\Report.wer	0	2	fd fd		success or wait	1	6E9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_88c9a135c9b22294e84c86e44fa262283b2da9a_82810a17_12540027\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	174	6E9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_88c9a135c9b22294e84c86e44fa262283b2da9a_82810a17_12540027\Report.wer	11720	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 37 00 31 00 39 00 31 00 30 00 36 00 37 00 34 00 37 00	MetadataHash=1719106747	success or wait	1	6E9D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6E9F36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6E9F1FB2	RegCreateKeyExW
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E9D43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LongPathHash	unicode	rundll32.exe\ab97b57a	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6E9F36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6E9F36BF	unknown
\REGISTRY\A\{38982dfb-1a08-ba7a-64bc-8c6ec4a428be}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6E9F36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	03 00 00 80 00 00 00 00 00 00 00 00 52 36 D9 6E 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6E9F1FE8	RegSetValueExW

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

Disassembly

No disassembly