ID: 564921
Sample Name: knigger.bin
Cookbook: default.jbs
Time: 15:41:40
Date: 02/02/2022
Version: 34.0.0 Boulder Opal

Table of Contents

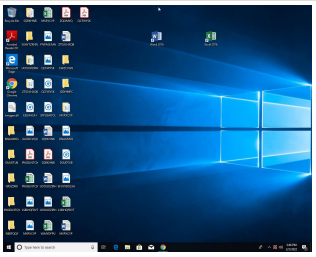
Windows Analysis Report

knigger.bin

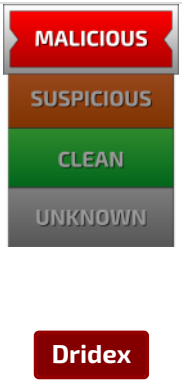
Overview

General Information

Sample Name:	knigger.bin (renamed file extension from bin to dll)
Analysis ID:	564921
MD5:	f2fdb0f416abda7..
SHA1:	cb35382ae44bc4..
SHA256:	5e5242e1251bfb..
Infos:	



Detection



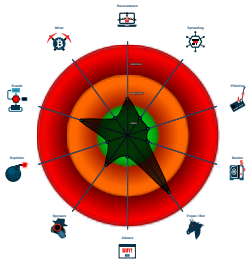
Dridex

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: 6348 cmdline: loaddll32.exe "C:\Users\user\Desktop\knigger.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6340 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\knigger.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6324 cmdline: rundll32.exe "C:\Users\user\Desktop\knigger.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 4680 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6324 -s 700 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
00000002.00000002.370345630.00000000011A0000.00000040.00000800.00020000.00000000.sdmp	MALWARE_Win_DLLLoader	Detects unknown DLL Loader	ditekSHen	• 0x3063:$s1: LondLibruryA • 0x304e:$s2: LdrLoadDll • 0x3059:$s3: snxhk.dll • 0x30f6:$s4: DisableThreadLibraryCalls
00000002.00000000.358193713.00000000011A0000.00000040.00000800.00020000.00000000.sdmp	MALWARE_Win_DLLLoader	Detects unknown DLL Loader	ditekSHen	• 0x3063:$s1: LondLibruryA • 0x304e:$s2: LdrLoadDll • 0x3059:$s3: snxhk.dll • 0x30f6:$s4: DisableThreadLibraryCalls
00000002.00000002.370546422.000000006F271000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000002.00000000.358345713.000000006F271000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000002.00000000.357246849.00000000011A0000.00000040.00000800.00020000.00000000.sdmp	MALWARE_Win_DLLLoader	Detects unknown DLL Loader	ditekSHen	• 0x3063:$s1: LondLibruryA • 0x304e:$s2: LdrLoadDll • 0x3059:$s3: snxhk.dll • 0x30f6:$s4: DisableThreadLibraryCalls
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.rundll32.exe.32fc63b.4.raw.unpack	MALWARE_Win_DLLLoader	Detects unknown DLL Loader	ditekSHen	• 0x1a93:$s1: LondLibruryA • 0x1a7e:$s2: LdrLoadDll • 0x1a89:$s3: snxhk.dll • 0x1b26:$s4: DisableThreadLibraryCalls
2.2.rundll32.exe.11a0000.0.raw.unpack	MALWARE_Win_DLLLoader	Detects unknown DLL Loader	ditekSHen	• 0x3063:$s1: LondLibruryA • 0x304e:$s2: LdrLoadDll • 0x3059:$s3: snxhk.dll • 0x30f6:$s4: DisableThreadLibraryCalls
2.2.rundll32.exe.11a0000.0.unpack	MALWARE_Win_DLLLoader	Detects unknown DLL Loader	ditekSHen	• 0x1a93:$s1: LondLibruryA • 0x1a7e:$s2: LdrLoadDll • 0x1a89:$s3: snxhk.dll • 0x1b26:$s4: DisableThreadLibraryCalls
2.0.rundll32.exe.32fc63b.1.unpack	MALWARE_Win_DLLLoader	Detects unknown DLL Loader	ditekSHen	• 0xcf3:$s1: LondLibruryA • 0xcde:$s2: LdrLoadDll • 0xce9:$s3: snxhk.dll • 0xd86:$s4: DisableThreadLibraryCalls
2.0.rundll32.exe.11a0000.3.raw.unpack	MALWARE_Win_DLLLoader	Detects unknown DLL Loader	ditekSHen	• 0x3063:$s1: LondLibruryA • 0x304e:$s2: LdrLoadDll • 0x3059:$s3: snxhk.dll • 0x30f6:$s4: DisableThreadLibraryCalls
Click to see the 10 entries				

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

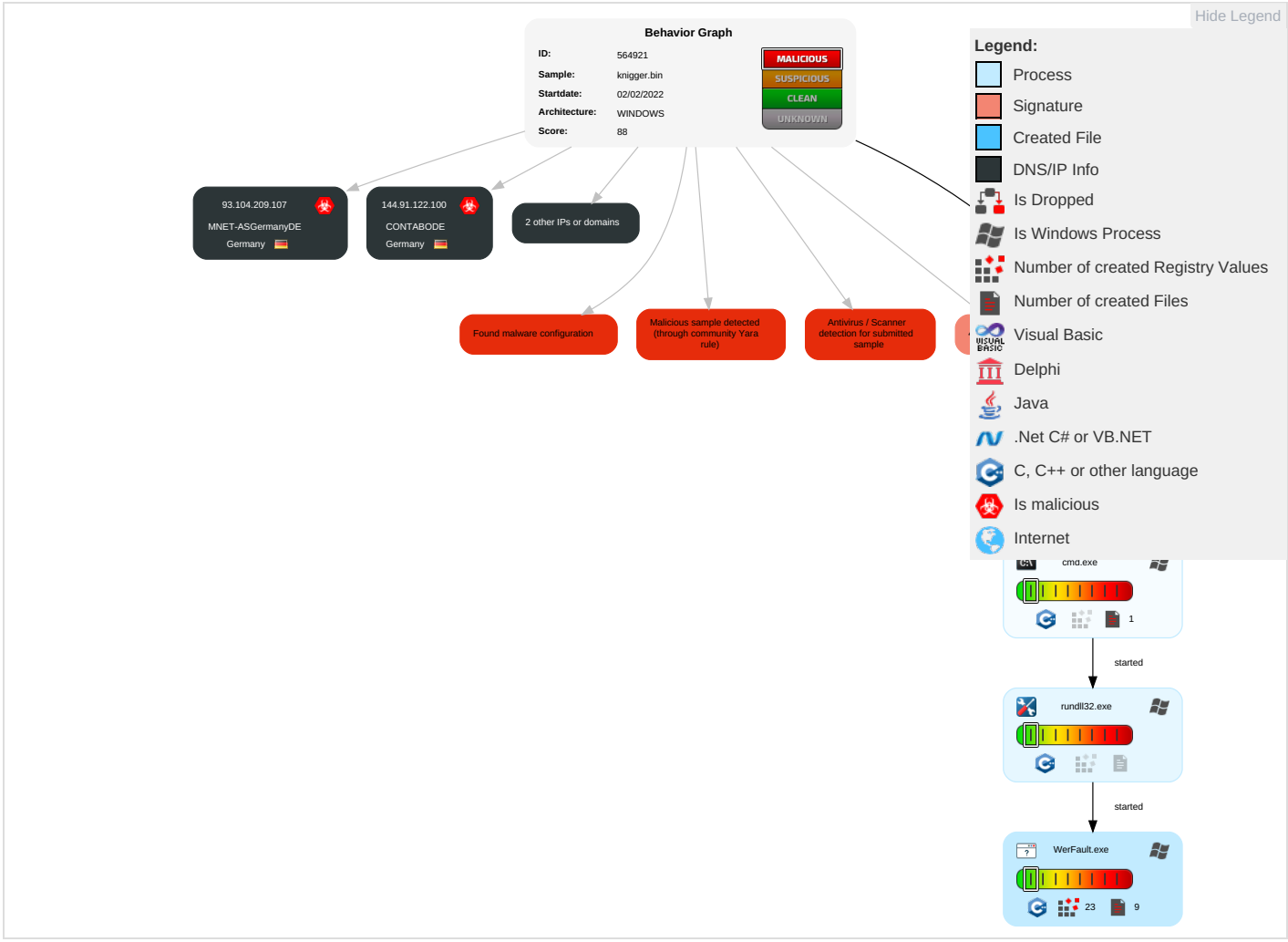
System Summary

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 Virtualization/Sandbox Evasion	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 Rundll32	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	Software Packing	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 1 System Information 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 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

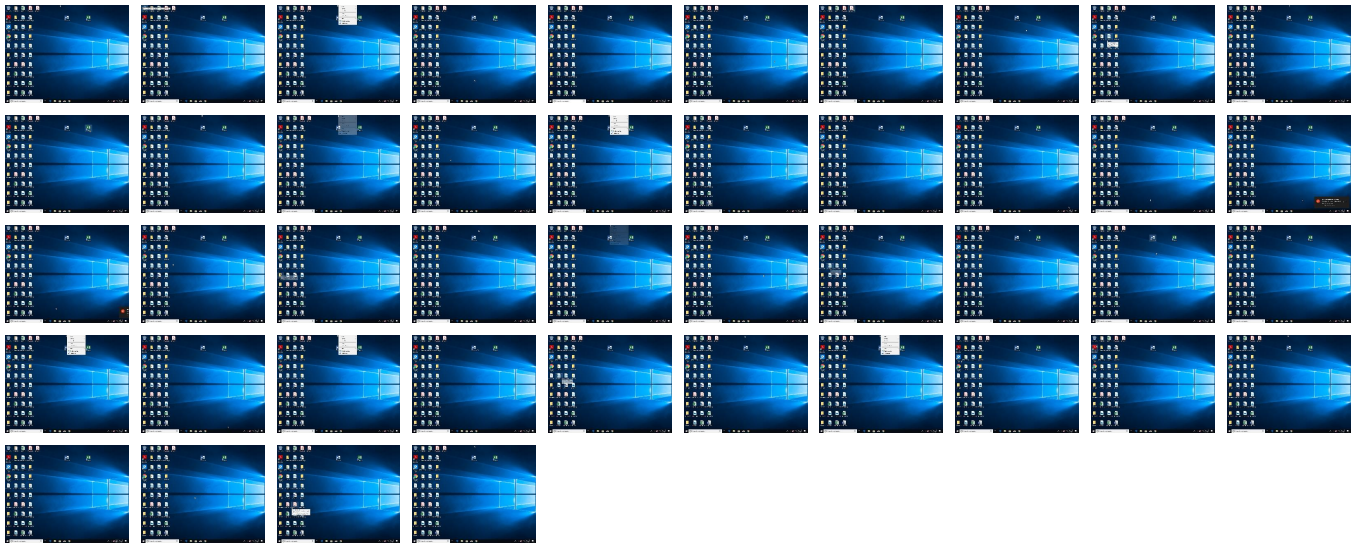
Behavior Graph



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	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
2.2.rundll32.exe.11a0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.rundll32.exe.6f270000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.6f270000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.6f270000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.11a0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
2.0.rundll32.exe.11a0000.3.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

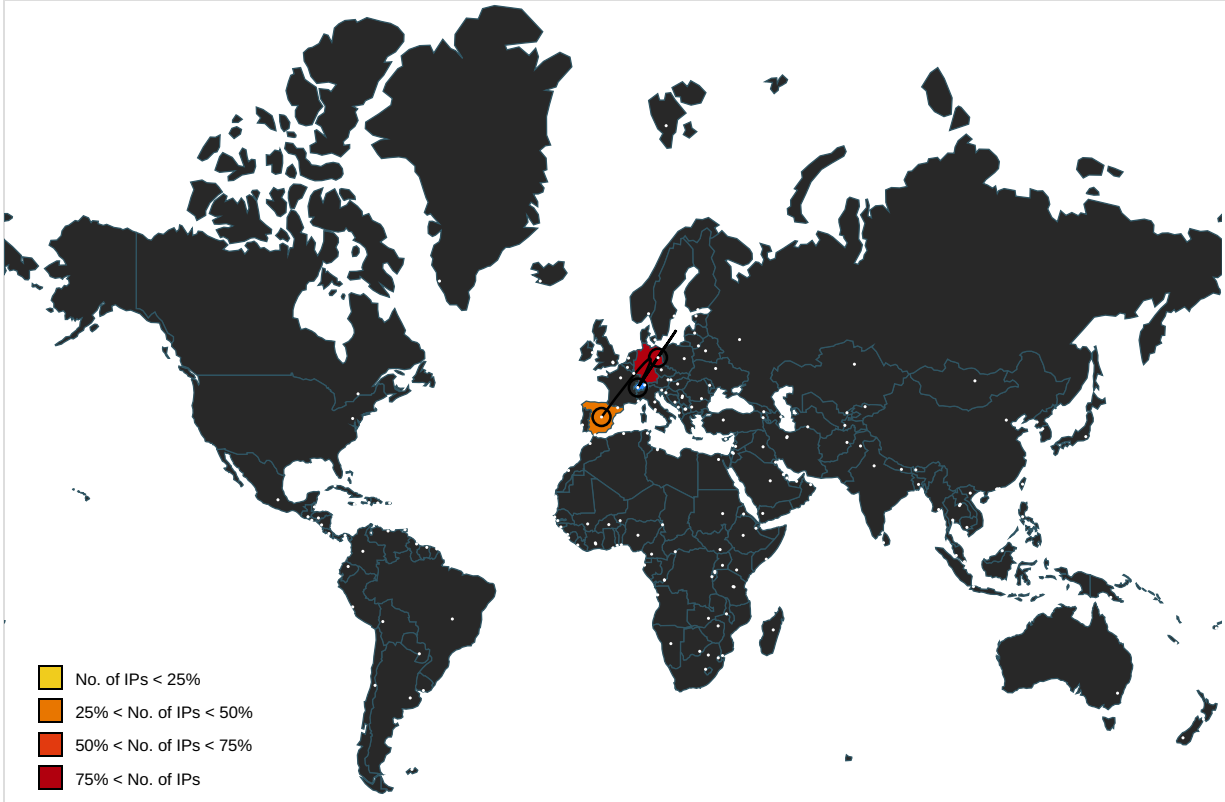
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://upx.sf.net	Amcache.hve.6.dr	false		high
http://www.kazanfirst.ruDVarFileInfo$	rundll32.exe, 00000002.00000000.3583731779.000000006F28F000.00000002.00000001.01000000.00000003.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:	15:41:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	knigger.bin (renamed file extension from bin to 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
Number of analysed new started processes analysed:	28
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@6/6@0/4
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 52.5% (good quality ratio 50.6%) • Quality average: 78.6% • Quality standard deviation: 27.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.54.113.53, 13.89.179.12
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, onedsblobprdcus17.centralus.cloudapp.azure.com, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.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
- VT rate limit hit for: knigger.dll

Simulations

Behavior and APIs

Time	Type	Description
15:42:50	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_88c9a135c9b22294e84c86e44fa262283b2da9a_82810a17_122904ea\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):	0.932361057778476
Encrypted:	false
SSDEEP:	192:6Vii0oXjHBUZMX4jed+P/u7spS274ItWc:cikXjBUZMX4jeq/u7spX4ItWc
MD5:	712EE66153C612FE2A7AA6FC985729BB
SHA1:	B2F7C3ECB750E05424B4C957D68274D3FBBBDF71
SHA-256:	CDC3F05FCC52A9B300B6900A17CB140EF99075A89FB41C31B2C096B8937432F1
SHA-512:	4780AB5BFCC7BB9379B1EF580AD1475A2437C7E8C3DB485E0698ACD07AB848B8584E9D77567DAD780E2EDF95CBB55995218DFDB5A93D1D13A568FC936683A52F
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.=.1.3.2.8.8.3.1.8.9.6.6.3.1.2.1.3.6.0.....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.=.1.3.2.8.8.3.1.8.9.6.9.1.0.9.0.0.2.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.8.3.f.9.4.c.c.-.6.0.b.c.-.4.d.9.9.-.9.5.8.2.-.3.7.5.6.8.b.b.b.b.2.6.d.....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.=.c.e.b.5.b.0.2.9.-.2.2.8.f.-.4.f.c.3.-.9.b.3.5.-.c.6.5.5.6.f.3.f.7.b.f.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.=.0.0.0.0.1.8.b.4.-.0.0.0.1.-.0.0.1.7.-.d.8.a.a.-.5.f.9.2.8.e.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\WERF4EC.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 2 23:42:46 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	45956
Entropy (8bit):	2.33754465661868
Encrypted:	false
SSDEEP:	192:5hQ/8qOnMzQDO5SkbV3bDu7EhWj8c+oAqBMt1na:Q2MF5LbVmj8cZAqaVa
MD5:	F4EE02EFEE8AD69BBF3A906A0C9CDF5F
SHA1:	BAD07B24B1C20FD5DBF3C176BD279A5807C2A330
SHA-256:	426F7F30254E664E414A1C1D610F2DA89CD567D7E0DC0A4BA1DE9B90EA210054
SHA-512:	1B030FA9F1B3A40939A588BE1BCA22A0D7AAC94FF63C20D8E8B0325A06927BBC42BB0D7EF38022F34A1C16F3C6DF3A98BC904BE2609FC471C55CB5CCCD91505
Malicious:	false
Reputation:	low

Preview:	MDMP..... .....a.....D.....T.....8.....T.....U.....B.....d.....GenuineIntelW.....T.....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\WERF8A6.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):	8240
Entropy (8bit):	3.689898444594183
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiqdS63b6R6YKw6WgmfTTSRCpra89b0visfR8m:RrlsNiqI6o6Yd6WgmfTTSK0vhf/
MD5:	F2DAD464F90154FCE75F0F86AAF8C0DF
SHA1:	D701FBBFB585419CA5C386089A3DE155B5D14786
SHA-256:	371924D06A753B50039AD1197442DDC28CBAC2A1E0BBFBFA0229ECA5562643B0
SHA-512:	89DC1C399C0D746BEC703CA6AA0F2C4A6DA71334C089A82D2BCB836C0E92EC24C14231AD7DEE036A2E3363699F5B8EF4D29D024479F69D8645FF901B74F4746
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.3.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA2E.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):	4.453834621245006
Encrypted:	false
SSDEEP:	48:cvIwSD8zsEJgtWI9g+WSC8B88fm8M4JCdsL2jGF78+q8/iKYR544SrS8d:uITfCP/SN/JJM34DW8d
MD5:	18872478B5333711926B37EA28B1C7AA
SHA1:	FC30FB7334320FF44049BBDF4A27A69E9D495E1E
SHA-256:	2D351F4C8F1D06A4B6B2F6EB7004280DB9A8D842D1CED83DD091C807EE312E50
SHA-512:	6BDA3227DAF90178636EC5603137BDE72BE6F665ADBE6EFCB24C1CADBCDE1770BB2D3A4AC96AD75B0A38E5F8EBEE0F2D7E610394ACC8589ACEE3C42D7913D200
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="1369973" />.. <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):	4.216496919713934
Encrypted:	false
SSDEEP:	12288:fDZIPRnLP6jV5jM72DlrIcK4UHjqYk/+t/lcST3kwdJOOcUP2dmbxT:rZIPRnLP6jzjM7cKDTHz
MD5:	F4CBF56A201641BE2B70F2F8AA40CCB0
SHA1:	01A55AA87EFDAC623087B552642C8B4163863EC1
SHA-256:	3B215E7FE68D246FD94F347E369FE24E9D71437CA782071395DB4F64D97F13D0
SHA-512:	3C863A393A5EDC7333F2C238CD7FA06D9AACF0443ABED6695EFCDBAEB45109313E7DA2BFFC871555FD71A1E1F9A032B04F3793740ABD3886AACE2C084A7A30AE
Malicious:	false

Reputation:	low
Preview:	regfV...V...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm..,..... ....'..... .....

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):	20480
Entropy (8bit):	3.5197824415151917
Encrypted:	false
SSDEEP:	384:Niy5NnIrnc8mTVgGFK0XnmnQFRiovOgIT:cMxAc8EVgGE0XmnQF9vP
MD5:	752FCD99E5EB7A9761D903827848FC50
SHA1:	AD9F5CF9EC6FB3670EAE8420B08D75059400BDBE
SHA-256:	53990467AC8208918CAEE7D1E2FA50D587F7B98BE48A621FFD148BD78B741BFD
SHA-512:	AF2359246FA2CF03FC7C0561BC37D74718E720972BA4D01A3FFB4D74DE524CF2D01B9CC3462F322884A556810FAEDDC373FF5E55B8D8D18A0FB9C9A517B549 7
Malicious:	false
Reputation:	low
Preview:	regfU...U...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm..,..... ....'.HvLE.N.....U.....9../#.....Hs4>.....`... ..hbin.....p.\..,.....nk,.eO/..... .....&...{ad79c032-a2ea-f756-e377- 72fb9332c3ae}.....nk .eO/..... ....Z.....Root.....lf.....Root....nk .eO/.....}..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck.....p...

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
add edx, 04h
call 00007F29B4DBD9A2h
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

Instruction
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]
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 00007F29B4DC1398h
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

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
.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

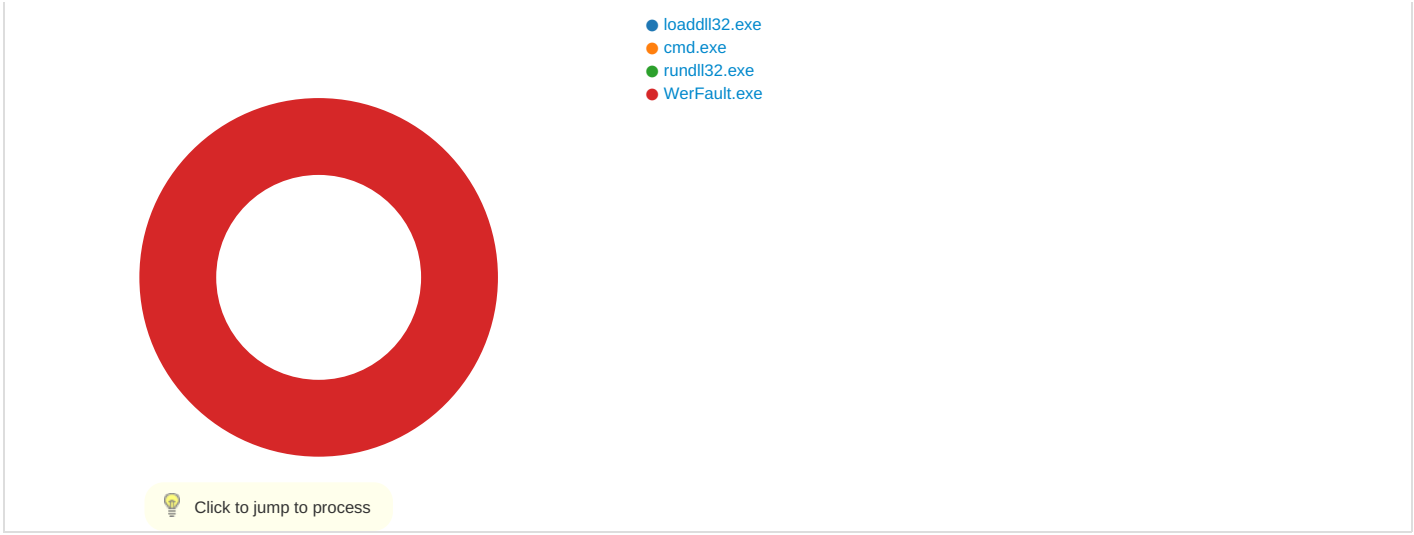
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **6348**, Parent PID: **4868**

General	
Target ID:	0
Start time:	15:42:42
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:	0x140000
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: **6340**, Parent PID: **6348**

General	
Target ID:	1
Start time:	15:42:42
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:	0x2a0000
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: 6324, Parent PID: 6340

General

Target ID:	2
Start time:	15:42:42
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:	0x1250000
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: 00000002.00000002.370345630.00000000011A0000.00000040.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_DLLLoader, Description: Detects unknown DLL Loader, Source: 00000002.00000000.358193713.00000000011A0000.00000040.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.370546422.000000006F271000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000000.358345713.000000006F271000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: MALWARE_Win_DLLLoader, Description: Detects unknown DLL Loader, Source: 00000002.00000000.357246849.00000000011A0000.00000040.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000000.357555659.000000006F271000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 4680, Parent PID: 6324

General

Target ID:	6
Start time:	15:42:45
Start date:	02/02/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6324 -s 700
Imagebase:	0x11a0000
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	6EED1717	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA2E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA2E.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_88c9a135c9b22294e84c86e44fa262283b2da9a_82810a17_122904ea	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_88c9a135c9b22294e84c86e44fa262283b2da9a_82810a17_122904ea\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EEC497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA2E.tmp	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp.dmp	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA2E.tmp.xml	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFAF7.tmp.csv	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE72.tmp.txt	success or wait	1	6EEC497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 16 fd 61 fd 05 12 00 00 00 00 00	MDMP a	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp.dmp	7780	6	00 00 00 00 00 00		success or wait	1	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.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 18 00 00 fd 16 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 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	UBdGenuineIntelWTa0=Pacific Standard TimePacific Daylight Time	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 04 01 00 00 28 fd 28 6f fd 06 fd 77 20 46 fd 77 fd 02 00 00 20 46 fd 77 00 00 00 00 52 36 28 6f 23 00 00 00 02 02 00 00 fd fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++((ow Fw FwR6(o#+	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp.dmp	1620	168	fd 18 00 00 00 00 00 00 03 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 52 36 28 6f 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 fd 02 00 00 fd 23 00 00	R6(o#	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp.dmp	12026	20	0f 00 00 00 fd fd 20 01 00 00 00 00 38 09 00 00 fd 2f 00 00	8/	success or wait	15	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp.dmp	12270	2360	fd fd fd 77 fd fd fd 77 64 02 00 00 fd fd fd fd 10 00 00 00 5c fd 20 01 28 fd 20 01 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd 00 70 fd 00 00 70 fd 00 00 00 00 00 64 02 00 00 fd fd fd fd 64 02 00 00 fd fd fd fd 00 70 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 04 3b 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd 06 3c 03 00 00 00 00 00 00 00 00 fd 06 3b 03 00 10 fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd 3c fd 2a 03 54 12 fd 00 44 fd 2a 03 20 05 3b 03 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwd\ (@w@wppddp;<; <*TD* ;	success or wait	14	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp.dmp	35742	256	56 fd 1e 4d fd fd fd 28 32 fd 39 fd fd fd fd fd fd fd 74 03 55 fd fd 5d d0 fd fd 56 56 fd 1e 4d fd fd fd fd fd 36 fd 6b fd fd fd fd 74 03 fd fd fd 33 fd d0 0f fd fd fd 10 fd fd fd 0f 4b fd d0 fd fd fd 4c 24 04 fd 03 00 00 00 fd fd fd 56 57 53 fd 28 fd 28 6f fd fd fd 3e fd 3c fd 74 22 68 68 fd fd 45 68 5c fd fd 60 fd 1b fd fd fd fd fd 74 09 57 6a 08 fd 36 fd fd fd 02 33 fd 5b 5f 5e fd 68 fd fd 6e 1c 68 5c fd fd 60 fd fd fd fd fd fd fd 68 fd fd 0a 5e 68 5c fd fd 60 fd fd fd fd fd fd 2c fd 28 6f fd 3e fd 3c fd 75 fd 33 fd 50 50 50 50 50 6a 02 fd c9 06 8b 44 24 04 0f fd 54 24 08 fd 4c 24 0c 57 53 55 fd fd fd fd 85 fd 74 24 fd fd 74 20 68 16 44 01 60 68 5c fd fd 60 fd fd fd fd fd 74 0d 55 0f fd fd 53 57 fd fd	VM(29tU]VVM6kt3L$VW S((o><t"hhE h\`tWj63[_^hnh\`h^h\`,(o> <u3PP PPPjD$T$L$WSUt$t hD`h\`tUSW	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.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 fd 00 00 00 00 20 46 fd 77 fd fd fd fd 00 00 00 00 58 fd fd 00 fd fd fd 77 23 00 00 00 02 02 00 00 fd fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++ FwXw#+	success or wait	3	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp.dmp	1888	48	10 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 70 fd 2a 03 00 00 00 00 fd 03 00 00 26 39 00 00 fd 02 00 00 2e 2c 00 00	p*&9.,	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp.dmp	1948	4	30 00 00 00	0	success or wait	48	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp.dmp	7028	752	00 00 48 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 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 fd fd 02 00 00 00 00 00 50 fd 02 00 00 00 00 7e 4b 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 65 fd 03 00 00 00 00 00 78 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 39 67 1b 00 00 00 00 00 07 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 04 00 00 00 00	Ht0Us@#BB? #@AZbP~Kex9g@	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.tmp.dmp	35998	9958	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	EventFileFile(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTim	success or wait	1	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4EC.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 fd 1b 00 00 17 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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6324</Pid>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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 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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 35 00 35 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4552</Uptime>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 37 00 33 00 33 00 31 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>128733184</PeakVirtualSize>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 38 00 34 00 36 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>2846</PageFaultCount>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 37 00 32 00 33 00 39 00 30 00 34 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>9723904</PeakWorkingSetSize>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 37 00 32 00 33 00 39 00 30 00 34 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>9723904</WorkingSetSize>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 32 00 33 00 31 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>182312</QuotaPagedPoolUsage>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 36 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 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>37616</QuotaPeakNonPagedPoolUsage>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 32 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>35232</QuotaNonPagedPoolUsage>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 34 00 39 00 36 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>6496256</PagefileUsage>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 34 00 39 00 36 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>6496256</PrivateUsage>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6340</Pid>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2904	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000 00000</Cm dLineSignature>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3006	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 38 00 37 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4877</Uptime>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3060	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3154	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3218	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3276	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>57405440</PeakVirtualSize>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3376	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 33 00 34 00 34 00 30 00 35 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>53440512</VirtualSize>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3460	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 32 00 30 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>1120</PageFaultCount>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3548	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 31 00 30 00 39 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3710976</PeakWorkingSetSize>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3658	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 39 00 38 00 36 00 38 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3698688</WorkingSetSize>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3752	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>40960</QuotaPeakPagedPoolUsage>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3878	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 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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	3988	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5632</QuotaPeakNonPagedPoolUsage>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4124	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>5224</QuotaNonPagedPoolUsage>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4244	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 30 00 31 00 36 00 30 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>3420160</PagefileUsage>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4334	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 37 00 31 00 37 00 31 00 32 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>3571712</PeakPagefileUsage>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4440	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 30 00 31 00 36 00 30 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>3420160</PrivateUsage>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4524	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4580	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4630	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4668	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4716	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4762	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	4832	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	5436	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	5440	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	5442	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	5482	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	5486	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	5488	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	5526	4	0d 00 0a 00		success or wait	6	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	5530	2	09 00		success or wait	12	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	5534	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6088	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6092	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6094	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6134	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6138	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6140	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6178	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6182	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6186	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6288	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 68 00 6d 00 65 00 63 00 65 00 6d 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>hmecem, Inc.</SystemManufacturer>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6402	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 68 00 6d 00 65 00 63 00 65 00 6d 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>hmecem7,1</SystemProductName>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6498	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6502	2	09 00		success or wait	2	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6506	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6626	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6630	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6634	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 39 00 33 00 36 00 30 00 34 00 37 00 32 00 31 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>1593604721</OSInstallDate>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6716	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6720	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6724	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6826	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6830	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6834	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6902	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6906	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6908	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6948	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6952	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6954	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6988	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6992	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	6996	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7092	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7096	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7098	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7134	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7138	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7140	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7164	4	0d 00 0a 00		success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7168	2	09 00		success or wait	6	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7172	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7418	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7422	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7424	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7450	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7454	2	09 00		success or wait	1	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7456	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 34 00 32 00 3a 00 34 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-02-02T23:42:47Z">	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7556	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7560	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7564	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 39 00 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 33 00 32 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 38 00 32 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 38 00 32 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="393" PID="6324" UptimeMS="828" TimeSinceCreationMS="828" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7822	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7826	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7830	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7856	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7894	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7898	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7900	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	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	7946	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 38 00 33 00 66 00 39 00 34 00 63 00 63 00 2d 00 36 00 30 00 62 00 63 00 2d 00 34 00 64 00 39 00 39 00 2d 00 39 00 35 00 38 00 32 00 2d 00 33 00 37 00 35 00 36 00 38 00 62 00 62 00 62 00 62 00 32 00 36 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>d83f94cc-60bc-4d99-9582-37568bbbb26d</Guid>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	8052	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 34 00 32 00 3a 00 34 00 37 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>2022-02-02T23:42:47Z</CreationTime>	success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	8156	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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	8196	4	0d 00 0a 00		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF8A6.tmp.WERInternalMetadata.xml	8200	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	6EEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA2E.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 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_88c9a135c9b22294e84c86e44fa262283b2da9a_82810a17_122904ea\Report.wer	0	2	fd fd		success or wait	1	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_88c9a135c9b22294e84c86e44fa262283b2da9a_82810a17_122904ea\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	6EEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_88c9a135c9b22294e84c86e44fa262283b2da9a_82810a17_122904ea\Report.wer	11724	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 34 00 35 00 35 00 34 00 39 00 32 00 36 00 33 00 31 00	MetadataHash=-455492631	success or wait	1	6EEC497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6EEE36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6EEE1FB2	RegCreateKeyExW
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EEC43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6EEE36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6EEE36BF	unknown
\REGISTRY\A\{0b841a5e-a088-d05c-585d-1a4e7d166f9e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6EEE36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
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 28 6F 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	6EEE1FE8	RegSetValueExW

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

Disassembly

No disassembly