ID: 594633
Sample Name: 555.exe
Cookbook: default.jbs
Time: 23:51:33
Date: 22/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

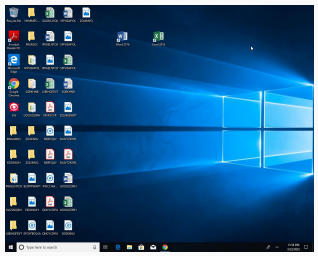
Windows Analysis Report

555.exe

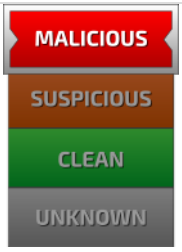
Overview

General Information

Sample Name:	555.exe
Analysis ID:	594633
MD5:	ed37ebbe1746dd.
SHA1:	0a559ebf6ab1cd..
SHA256:	b4c9aadd18c1b6..
Tags:	ArkeiStealer exe Vidar
Infos:	



Detection



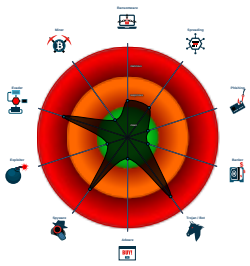
Oski Stealer Vidar

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Oski Stealer
- Antivirus / Scanner detection for sub…
- Yara detected Vidar stealer
- Multi AV Scanner detection for dom…
- Injects a PE file into a foreign proce…
- Country aware sample found (crashe…
- Found many strings related to Crypt…
- Uses 32bit PE files
- Yara signature match
- One or more processes crash

Classification



Process Tree

- **System is w10x64**
- 555.exe (PID: 6192 cmdline: "C:\Users\user\Desktop\555.exe" MD5: ED37EBBE1746DD0D566C8C4769655E0B)
  - 555.exe (PID: 6444 cmdline: C:\Users\user\Desktop\555.exe MD5: ED37EBBE1746DD0D566C8C4769655E0B)
    - WerFault.exe (PID: 6864 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6444 -s 1228 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.292388271.00000000048A5000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Oski_1	Yara detected Oski Stealer	Joe Security	
00000000.00000002.292388271.00000000048A5000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000003.00000000.294887526.0000000000474000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_Oski_1	Yara detected Oski Stealer	Joe Security	
00000003.00000000.294887526.0000000000474000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000000.00000002.291455838.00000000047B2000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Oski_1	Yara detected Oski Stealer	Joe Security	

Click to see the 15 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.555.exe.400000.4.raw.unpack	JoeSecurity_Oski_1	Yara detected Oski Stealer	Joe Security	
3.0.555.exe.400000.4.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
3.0.555.exe.400000.4.raw.unpack	Vidar	Vidar Payload	kevoreilly	• 0x1056:$decode: FF 75 0C 8D 34 1F FF 15 9C 41 47 00 8B C8 33 D2 8B C7 F7 F1 8B 45 0C 8B 4D 08 8A 04 02 32 04 31 47 88 06 3B 7D 10 72 D8 • 0x75b10:$wallet: *walle*.dat
3.2.555.exe.400000.0.unpack	JoeSecurity_Oski_1	Yara detected Oski Stealer	Joe Security	
3.2.555.exe.400000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 1 entries				

Sigma Signatures

There are no malicious signatures, click here to show all signatures.

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Country aware sample found (crashes after keyboard check)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Oski Stealer

Yara detected Vidar stealer

Found many strings related to Crypto-Wallets (likely being stolen)

Remote Access Functionality

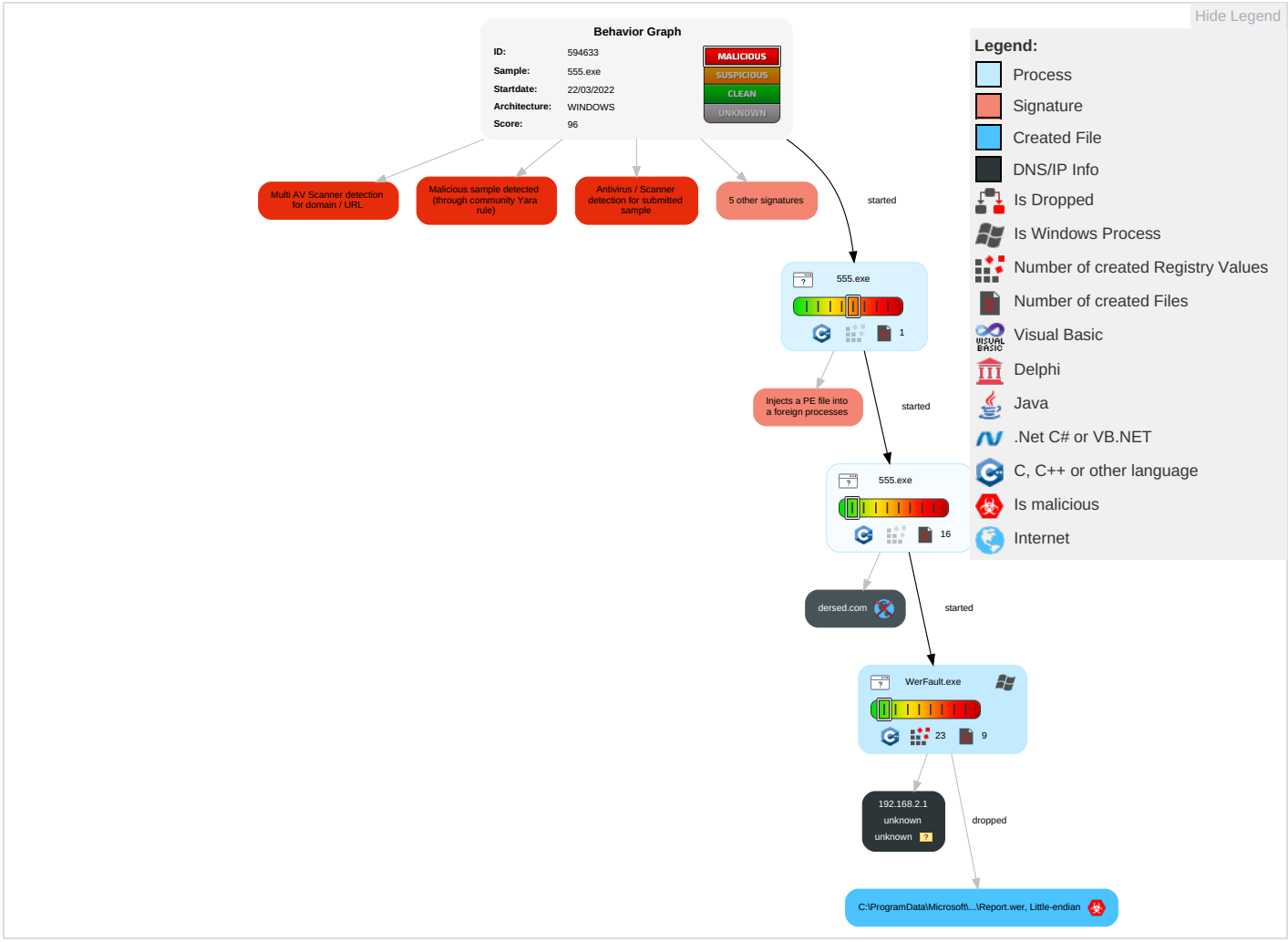
Yara detected Oski Stealer

Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	1 1 1 Process Injection	1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 Network Share Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 1 Process Injection	LSASS Memory	1 2 System Time Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	3 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Virtualization/Sandbox Evasion	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	2 Process 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 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 Account Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	2 File and Directory Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	2 6 System Information Discovery	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

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
555.exe	71%	Virustotal		Browse
555.exe	41%	Metadefender		Browse
555.exe	79%	ReversingLabs	Win32.Trojan.Graftor	
555.exe	100%	Avira	HEUR/AGEN.1206114	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.555.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1206114		Download File
3.2.555.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1210209		Download File
0.0.555.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1206114		Download File
0.2.555.exe.712ed8.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
dersed.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://dersed.com/freebl3.dll	5%	Virustotal		Browse
http://dersed.com/freebl3.dll	0%	Avira URL Cloud	safe	
http://dersed.com/nss3.dllv	0%	Avira URL Cloud	safe	
http://dersed.com/vcruntime140.dllbg	0%	Avira URL Cloud	safe	
http://dersed.com/288	0%	Avira URL Cloud	safe	
http://dersed.com/vcruntime140.dll	0%	Avira URL Cloud	safe	
http://dersed.com/softokn3.dllUD	0%	Avira URL Cloud	safe	
http://dersed.com/vcruntime140.dll_i	0%	Avira URL Cloud	safe	
http://dersed.com/msvcp140.dllGD	0%	Avira URL Cloud	safe	
http://dersed.com/softokn3.dllmb	0%	Avira URL Cloud	safe	
http://dersed.com/msvcp140.dll	0%	Avira URL Cloud	safe	
http://dersed.com/nss3.dll	0%	Avira URL Cloud	safe	
http://dersed.com/mozglue.dll	0%	Avira URL Cloud	safe	
http://dersed.com/softokn3.dllLD	0%	Avira URL Cloud	safe	
http://dersed.com/freebl3.dllyD	0%	Avira URL Cloud	safe	
http://dersed.com/mozglue.dllkD	0%	Avira URL Cloud	safe	
http://dersed.com/nss3.dllcom/freebl3.dll	0%	Avira URL Cloud	safe	
http://dersed.com/softokn3.dll	0%	Avira URL Cloud	safe	
http://dersed.com/vcruntime140.dllGc	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

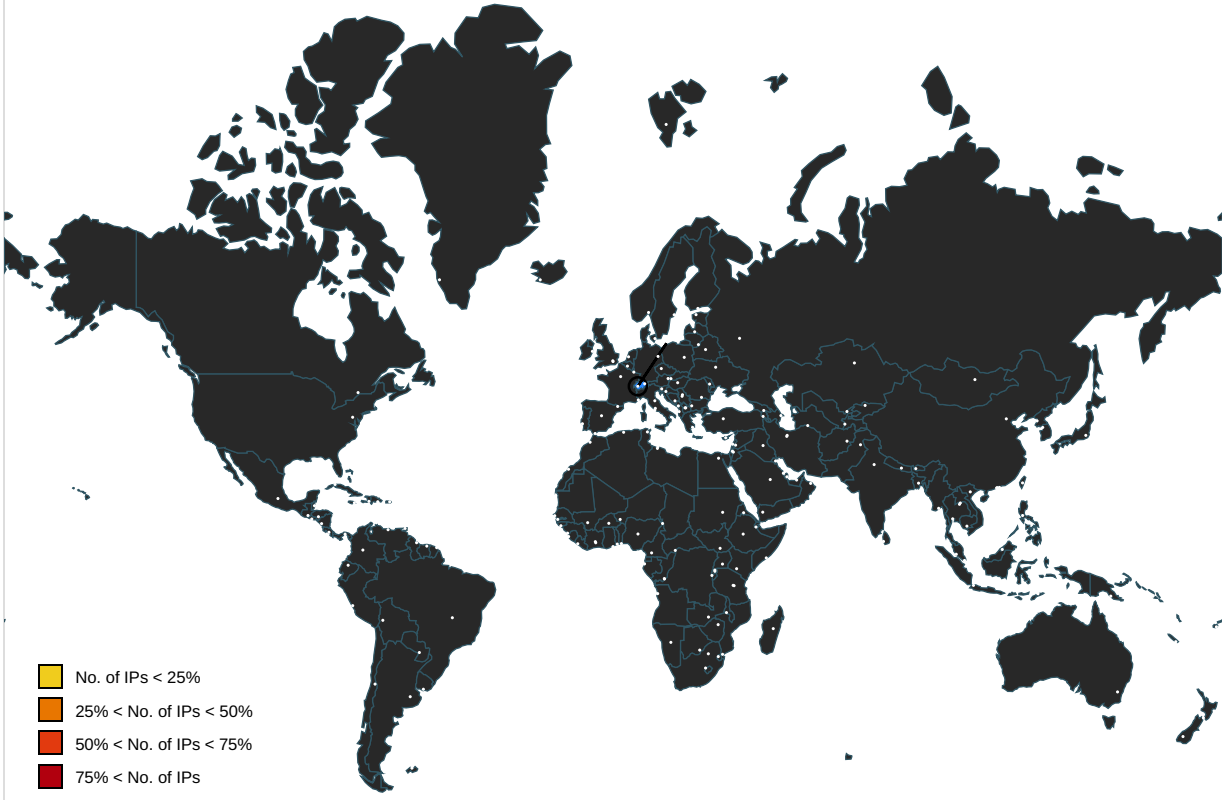
Name	IP	Active	Malicious	Antivirus Detection	Reputation
dersed.com	unknown	unknown	false	• 4%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://dersed.com/freebl3.dll	555.exe, 00000003.00000002.317565007.000 0000000836000.00000004.00000020.00020000 .00000000.sdmp	true	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://dersed.com/nss3.dllv	555.exe, 00000003.00000002.317520983.000 00000007E7000.00000004.00000020.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dersed.com/vcruntime140.dllbg	555.exe, 00000003.00000002.317555951.000 0000000826000.00000004.00000020.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dersed.com/288	555.exe, 00000003.00000002.317520983.000 00000007E7000.00000004.00000020.00020000 .00000000.sdmp, 555.exe, 00000003.000000 02.317555951.0000000000826000.00000004.0 0000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dersed.com/vcruntime140.dll	555.exe, 00000003.00000002.317555951.000 0000000826000.00000004.00000020.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dersed.com/softokn3.dllUD	555.exe, 00000003.00000002.317565007.000 0000000836000.00000004.00000020.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dersed.com/vcruntime140.dll_i	555.exe, 00000003.00000002.317555951.000 0000000826000.00000004.00000020.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dersed.com/msvcp140.dllGD	555.exe, 00000003.00000002.317565007.000 0000000836000.00000004.00000020.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://dersed.com/softokn3.dllmb	555.exe, 00000003.00000002.317555951.0000000826000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dersed.com/msvcp140.dll	555.exe, 00000003.00000002.317565007.0000000836000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dersed.com/nss3.dll	555.exe, 00000003.00000002.317520983.00000007E7000.00000004.00000020.00020000.00000000.sdmp, 555.exe, 00000003.00000002.317555951.0000000000826000.00000004.00000020.00020000.00000000.sdmp, 555.exe, 00000003.00000002.317565007.0000000000836000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dersed.com/mozglue.dll	555.exe, 00000003.00000002.317565007.0000000836000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dersed.com/softokn3.dllLD	555.exe, 00000003.00000002.317565007.0000000836000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dersed.com/freebl3.dllyD	555.exe, 00000003.00000002.317565007.0000000836000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://dersed.com/mozglue.dllkD	555.exe, 00000003.00000002.317565007.0000000836000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dersed.com/nss3.dllcom/freebl3.dll	555.exe, 00000003.00000002.317565007.0000000836000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ip-api.com/line/	555.exe, 00000003.00000000.288286831.0000000400000.00000004.00000001.01000000.00000003.sdmp	false		high
http://dersed.com/softokn3.dll	555.exe, 00000003.00000002.317555951.0000000826000.00000004.00000020.00020000.00000000.sdmp, 555.exe, 00000003.00000002.317565007.0000000000836000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dersed.com/vcruntime140.dllGc	555.exe, 00000003.00000002.317555951.0000000826000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	594633
Start date and time:	2022-03-22 22:51:33 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	555.exe
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:	26
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:	mal96.troj.spyw.evad.winEXE@4/4@7/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 96% (good quality ratio 85.8%) • Quality average: 70.5% • Quality standard deviation: 33.1%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 20.189.173.20, 20.54.110.249
- Excluded domains from analysis (whitelisted): fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, onedsblobprdwus15.westus.cloudapp.azure.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
23:53:15	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_555.exe_73a2317c9b18c06fb4572ea77cd525ee3f28dbd_69550887_1ab655c1\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):	0.9430986111528993
Encrypted:	false
SSDEEP:	192:M2AFk0lk4YHBUZMXojAK3Yw/u7shS274Itx:QPlk9BUZMXojL/u7shX4Itx
MD5:	9B8FC50DD0D29F54F499621D50C8AD62
SHA1:	1273BFD6929FB2B4CA4874A792AE69816B1E2F11
SHA-256:	9655AA68E28BDC15B2CBB4DAA13850F1A086D82D45FF56F78C3FEEE8A0CBF803
SHA-512:	BFC071EAB661547CB0BD88D00ECBBEF817CF30CF4A9ACBCAEFF1BFB1569075424335948962E71C07F5360BC53316DCF1687D9CF46278F62EC1F89128B49EAE95
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.2.4.6.3.1.8.9.2.9.4.5.4.9.0.....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.=.1.3.2.9.2.4.6.3.1.9.4.0.4.4.5.0.0.6.....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.=.a.f.b.1.4.f.5.b.-.8.2.8.0.-.4.5.a.e.-.b.e.e.9.-.7.5.f.a.d.4.b.7.9.6.4.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.d.2.3.d.f.d.7.-.1.7.0.6.-.4.7.b.5.-.9.3.4.9.-.d.c.5.f.9.a.f.9.a.e.2.6.....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.=.5.5.5...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.2.c.-.0.0.0.1.-.0.0.1.c.-.7.9.3.2.-.0.8.9.4.3.f.3.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.5.d.f.1.3.d.4.1.7.b.e.7.e.f.d.1.d.6.5.0.9.b.f.e.9.4.7.4.8.5.3.9.0.0.0.0.0.9.0.4.!.0.0.0.0.0.a.5.5.9.e.b.f.6.a.b.1.c.d.f.2.9.2.c.7.9.a.a.c.5.a.c.2.0.c.2.3.6.d.9.7.5.e.b.7.!.5.5.5...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.1.9././.0.9././.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Mar 22 22:53:11 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	92494
Entropy (8bit):	1.9553236387916726
Encrypted:	false
SSDEEP:	384:HvVcEVMCcx960PIEQUnVT9sEQOeYBF+D+2IYBO:HyChQI5gVKE4YBF+x6
MD5:	87D9B100A994FF000B5C06267BE0226D

SHA1:	46D41AFA9086777230CB38F7F957024E34F57815
SHA-256:	258E97FE2FC99EE493D3F78937B42C864BBA2654D5348A464FC129E83F464970
SHA-512:	F4CE8D98D9AF8FAF155BDBC3BB62E35D74B558465F79D520ACB009747F669CC50CEE20772B0DC326E96AA5DA322DAC4808831FAA4C8598D48AF45EADC96ED A73
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....WS:b.....D.....T.....8.....T.....x...:.....U.....B..... .....GenuineIn telW.....T.....,..KS:b.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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):	8234
Entropy (8bit):	3.688431082756376
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWN6Irwt6Yei6DgmfhhS8+pr589bWTsf0Oym:RrlsNi06IrS6Yj6DgmfnSGW4fv
MD5:	CDE05209CC74B1005E7AD76327AA3173
SHA1:	651DF6AA11E2B4F6CDF1E21A1228A0FF68CD0743
SHA-256:	ABB9D8C4C33EEC5B9D10B346747AE37C70F8F58CCDC7D12984A467C0A4AE4531
SHA-512:	19AB7546E950373EC778423E45C2D08718D9C5525182D14F42CC2F2082A10247515AE4728541736B8453A7B3A277DAA4602BC77E0B15C60C65C9D3F9CE33C0E9
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.>.6.4.4. 4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4E21.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4522
Entropy (8bit):	4.423325556237254
Encrypted:	false
SSDEEP:	48:cvIwSD8zskJgtWI9NJWgc8sqYjK8fm8M4J61RF3I+q8mbwhHXSrxd:uITfia4grsqYrJ69I/wxSrxd
MD5:	68930925340EA9386F5C57115BC56C4A
SHA1:	21FFD5E3BDD640870D896B69AB35C588364B5611
SHA-256:	F6AA5BD71759921218656247A52D2CE89A6BA9F53F4AFB7BBB1A79E45A369E5D
SHA-512:	7E78820E9C2427F020176D43CFBCF73E6785E7E67E08F79EB317E69493D27D63E2F2FE8915B02117097B95A46F350C56177A81DBDA067472424BBC72CD7663E5
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="1439043" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.692192927991023

TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	555.exe
File size:	1304576
MD5:	ed37ebbe1746dd0d566c8c4769655e0b
SHA1:	0a559ebf6ab1cdf292c79aac5ac20c236d975eb7
SHA256:	b4c9aadd18c1b6f613bf9d6db71dcc010bbdfe8b770b4084eeb7d5c77d95f180
SHA512:	aed30ae2e22ded5374f56062cdbcc2a72edea1d727e7fd0624e627f363d18787d5ce4334066b76b23d10e0a2c0169f06e5d6a8f05037d0943bfea110ee805060
SSDEEP:	24576:atLyuIJLGWVpPq48nuzldzB2sZL7kHNWDzBHc6ewxl:KLgFGYq48nupdzB2sp7kHNW51eE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.....H...H...H..iH...H..]Hc..H.`tH...H.`dH...H...H...H..\H...H..mH...H..jH...HRich...H.....PE..L...t.q]...

File Icon

Icon Hash:	18f0f8d2f2e4f206

Static PE Info

General

Entrypoint:	0x424e16
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5D710174 [Thu Sep 5 12:37:08 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	5f3146513f84438aa6d693baf35ebf34

Entrypoint Preview

Instruction
call 00007FAC08A60E69h
jmp 00007FAC08A5841Eh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
test eax, eax
je 00007FAC08A585A4h
sub eax, 08h
cmp dword ptr [eax], 0000DDDDh
jne 00007FAC08A58599h
push eax
call 00007FAC08A56352h
pop ecx
pop ebp
ret
mov edi, edi
push ebp

Instruction
mov ebp, esp
sub esp, 10h
mov eax, dword ptr [004608E0h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
mov edx, dword ptr [ebp+18h]
push ebx
xor ebx, ebx
push esi
push edi
cmp edx, ebx
jle 00007FAC08A585B1h
mov eax, dword ptr [ebp+14h]
mov ecx, edx
dec ecx
cmp byte ptr [eax], bl
je 00007FAC08A5859Ah
inc eax
cmp ecx, ebx
jne 00007FAC08A58588h
or ecx, FFFFFFFFh
mov eax, edx
sub eax, ecx
dec eax
cmp eax, edx
jnl 00007FAC08A58593h
inc eax
mov dword ptr [ebp+18h], eax
mov dword ptr [ebp-08h], ebx
cmp dword ptr [ebp+24h], ebx
jne 00007FAC08A5859Dh
mov eax, dword ptr [ebp+08h]
mov eax, dword ptr [eax]
mov eax, dword ptr [eax+04h]
mov dword ptr [ebp+24h], eax
mov esi, dword ptr [00451204h]
xor eax, eax
cmp dword ptr [ebp+28h], ebx
push ebx
push ebx
push dword ptr [ebp+18h]
setne al
push dword ptr [ebp+14h]
lea eax, dword ptr [00000001h+eax*8]
push eax
push dword ptr [ebp+24h]
call esi
mov edi, eax
mov dword ptr [ebp-10h], edi
cmp edi, ebx
jne 00007FAC08A58599h
xor eax, eax
jmp 00007FAC08A586E7h
jle 00007FAC08A585D5h
push FFFFFFE0h
xor edx, edx
pop eax
div edi
cmp eax, 02h

Instruction
jc 00007FAC08A585C9h
lea eax, dword ptr [edi+edi+08h]
cmp eax, 00000400h
jnbe 00007FAC08A585A5h
call 00007FAC08A58644h

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [LNK] VS2010 SP1 build 40219 • [ASM] VS2010 SP1 build 40219 • [RES] VS2010 SP1 build 40219 • [C] VS2010 SP1 build 40219 • [C++] VS2010 SP1 build 40219 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x5e954	0x12c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x66000	0xdd458	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x57690	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x51000	0x364	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4f7d9	0x4f800	False	0.48689010908	data	6.55171601636	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x51000	0xeca4	0xee00	False	0.418723739496	data	5.42402682187	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x60000	0x58c4	0x2800	False	0.26943359375	data	4.43475879322	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x66000	0xdd458	0xdd600	False	0.962993188876	data	7.93995191617	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AFX	0x6673c	0x10218	data	English	United States
CUSTOM	0x76954	0x36f3e	data	English	United States
RCDATA	0xad894	0x894ac	data	English	United States
RT_ICON	0x136d40	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x13af68	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x13d510	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x13e5b8	0x988	data	English	United States
RT_ICON	0x13ef40	0x468	GLS_BINARY_LSB_FIRST	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x13f3a8	0x70	data	English	United States
RT_DIALOG	0x13f418	0x224	data	English	United States
RT_DIALOG	0x13f63c	0x390	data	English	United States
RT_DIALOG	0x13f9cc	0x172	data	English	United States
RT_DIALOG	0x13fb40	0xe2	data	English	United States
RT_DIALOG	0x13fc24	0xf8	data	English	United States
RT_DIALOG	0x13fd1c	0x24c	data	English	United States
RT_STRING	0x13ff68	0xb98	data	English	United States
RT_STRING	0x140b00	0x2a	data	English	United States
RT_STRING	0x140b2c	0x1a4	data	English	United States
RT_STRING	0x140cd0	0xda	data	English	United States
RT_STRING	0x140dac	0x384	data	English	United States
RT_STRING	0x141130	0x38c	data	English	United States
RT_STRING	0x1414bc	0x140	data	English	United States
RT_STRING	0x1415fc	0x71c	data	English	United States
RT_STRING	0x141d18	0x638	data	English	United States
RT_STRING	0x142350	0xe8	data	English	United States
RT_STRING	0x142438	0x4a8	data	English	United States
RT_STRING	0x1428e0	0x38c	data	English	United States
RT_STRING	0x142c6c	0x62	data	English	United States
RT_STRING	0x142cd0	0x13c	data	English	United States
RT_STRING	0x142e0c	0x3a	data	English	United States
RT_GROUP_ICON	0x142e48	0x4c	data	English	United States
RT_VERSION	0x142e94	0x338	data	English	United States
RT_MANIFEST	0x1431cc	0x28a	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetTimeFormatA, GetProcessHeap, SetEndOfFile, CreateFileW, SetEnvironmentVariableA, CompareStringW, SetStdHandle, WriteConsoleW, LoadLibraryW, IsValidLocale, EnumSystemLocalesA, GetLocaleInfoA, GetUserDefaultLCID, HeapReAlloc, GetLocaleInfoW, GetStringTypeW, GetSystemTimeAsFileTime, GetCurrentProcessId, GetTickCount, GetDateFormatA, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetModuleFileNameA, GetModuleFileNameW, FlushFileBuffers, GetConsoleMode, GetConsoleCP, GetFileType, InitializeCriticalSectionAndSpinCount, lstrlenW, SetHandleCount, HeapSize, IsValidCodePage, GetOEMCP, GetACP, IsDebuggerPresent, SetUnhandledExceptionFilter, UnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, GetTempPathA, GetTempFileNameA, GetFinalPathNameByHandleA, GetLastError, CreateFileA, GetFileSize, SetFilePointer, ReadFile, CloseHandle, lstrcpyW, GetCurrentDirectoryW, VirtualQuery, QueryPerformanceCounter, lstrcpyA, WideCharToMultiByte, MulDiv, GlobalAlloc, ExitProcess, SizeofResource, LoadResource, LockResource, GetCurrentThreadId, SetLastError, GetModuleHandleW, TlsFree, TlsSetValue, TlsGetValue, TlsAlloc, HeapCreate, IsProcessorFeaturePresent, HeapAlloc, GetCPInfo, LCMapStringW, GetTimeZoneInformation, GetStartupInfoW, HeapSetInformation, GetCommandLineA, RtlUnwind, RaiseException, FindResourceA, LoadLibraryA, HeapFree, DecodePointer, EncodePointer, GetProcAddress, WriteFile, lstrcatA, GetLocalTime, GetTimeFormatW, GetDateFormatW, GetStdHandle, GetModuleHandleA, LeaveCriticalSection, EnterCriticalSection, DeleteCriticalSection, InitializeCriticalSection, Sleep, MultiByteToWideChar, InterlockedExchange, InterlockedCompareExchange, InterlockedDecrement, InterlockedIncrement
USER32.dll	SendMessageW, PostQuitMessage, DefWindowProcA, LoadBitmapA, DefDlgProcA, ClientToScreen, SendMessageA, CreateWindowExA, InsertMenuItemA, ShowWindow, HideCaret, WindowFromPoint, EnableWindow, UnionRect, SetRect, SetActiveWindow, GetWindowLongA, GetForegroundWindow, IsZoomed, SetWindowPos, GetSystemMetrics, GetWindowRect, EnumChildWindows, PostMessageA, RegisterClassA, SendDlgItemMessageA, GetParent, EndPaint, DrawTextA, GetClientRect, BeginPaint, GetDlgItem, LoadIconA, LoadCursorA, SetWindowLongA, CreateMenu, AppendMenuA, UpdateWindow, GetMessageA, TranslateMessage, DispatchMessageA, IsWinEventHookInstalled, GetActiveWindow
GDI32.dll	CreateFontA, SelectObject, DeleteObject, SetBkMode, CreateFontW, CreateFontIndirectA, TextOutA, StartPage, GetTextMetricsW, GetTextExtentExPointW, ExtTextOutW, EndPage, SetStretchBltMode, GetStockObject
COMDLG32.dll	CommDlgExtendedError, GetSaveFileNameA, ChooseFontA
ADVAPI32.dll	LsaRemoveAccountRights, LsaAddAccountRights
ole32.dll	CoInitialize, CreateBindCtx, MkParseDisplayName
WS2_32.dll	WSACreateEvent, WSAWaitForMultipleEvents
NETAPI32.dll	NetApiBufferFree, NetUserEnum
WINMM.dll	midiInOpen, midiInGetDevCapsA, PlaySoundA, midiInStart, mmioDescend, mmioSeek, midiInClose, mmioClose, midiInGetNumDevs
CRYPT32.dll	CertEnumPhysicalStore
SHLWAPI.dll	SHAutoComplete, PathCompactPathA
COMCTL32.dll	ImageList_GetImageCount, ImageList_LoadImageA, ImageList_Add, ImageList_DragMove, _TrackMouseEvent, ImageList_Create

DLL	Import
gdiplus.dll	GdiplusStartup, GdipCloneImage, GdipFree, GdipDeleteGraphics, GdipLoadImageFromFile, GdipDrawImageRectRectI, GdipAlloc, GdipDisposeImage, GdipGetImageWidth, GdipGetImageHeight, GdipCreateFromHDC, GdipSetInterpolationMode
UxTheme.dll	OpenThemeData

Version Infos

Description	Data
LegalCopyright	Bitdefender LLC Copyright . All rights reserved.
CompanyName	Bitdefender LLC
FileDescription	Selfssl Progresses Fatherbard New
Comments	Selfssl Progresses Fatherbard New
ProductName	Cnnmgrestablishcnnectin283715
ProductVersion	8.2.5.127
PrivateBuild	8.2.5.127
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 22, 2022 23:53:04.067533016 CET	60758	53	192.168.2.4	8.8.8.8
Mar 22, 2022 23:53:04.095592022 CET	53	60758	8.8.8.8	192.168.2.4
Mar 22, 2022 23:53:04.115511894 CET	60647	53	192.168.2.4	8.8.8.8
Mar 22, 2022 23:53:04.136682034 CET	53	60647	8.8.8.8	192.168.2.4
Mar 22, 2022 23:53:04.145426989 CET	64909	53	192.168.2.4	8.8.8.8
Mar 22, 2022 23:53:04.171823978 CET	53	64909	8.8.8.8	192.168.2.4
Mar 22, 2022 23:53:04.218432903 CET	60381	53	192.168.2.4	8.8.8.8
Mar 22, 2022 23:53:04.240736008 CET	53	60381	8.8.8.8	192.168.2.4
Mar 22, 2022 23:53:04.260018110 CET	56509	53	192.168.2.4	8.8.8.8
Mar 22, 2022 23:53:04.281152964 CET	53	56509	8.8.8.8	192.168.2.4
Mar 22, 2022 23:53:04.305391073 CET	54069	53	192.168.2.4	8.8.8.8
Mar 22, 2022 23:53:04.324481010 CET	53	54069	8.8.8.8	192.168.2.4
Mar 22, 2022 23:53:04.335752964 CET	57747	53	192.168.2.4	8.8.8.8
Mar 22, 2022 23:53:04.354562044 CET	53	57747	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 22, 2022 23:53:04.067533016 CET	192.168.2.4	8.8.8.8	0x8694	Standard query (0)	dersed.com	A (IP address)	IN (0x0001)
Mar 22, 2022 23:53:04.115511894 CET	192.168.2.4	8.8.8.8	0xeb1c	Standard query (0)	dersed.com	A (IP address)	IN (0x0001)
Mar 22, 2022 23:53:04.145426989 CET	192.168.2.4	8.8.8.8	0x99f3	Standard query (0)	dersed.com	A (IP address)	IN (0x0001)
Mar 22, 2022 23:53:04.218432903 CET	192.168.2.4	8.8.8.8	0x774b	Standard query (0)	dersed.com	A (IP address)	IN (0x0001)
Mar 22, 2022 23:53:04.260018110 CET	192.168.2.4	8.8.8.8	0x764c	Standard query (0)	dersed.com	A (IP address)	IN (0x0001)
Mar 22, 2022 23:53:04.305391073 CET	192.168.2.4	8.8.8.8	0x2f6	Standard query (0)	dersed.com	A (IP address)	IN (0x0001)

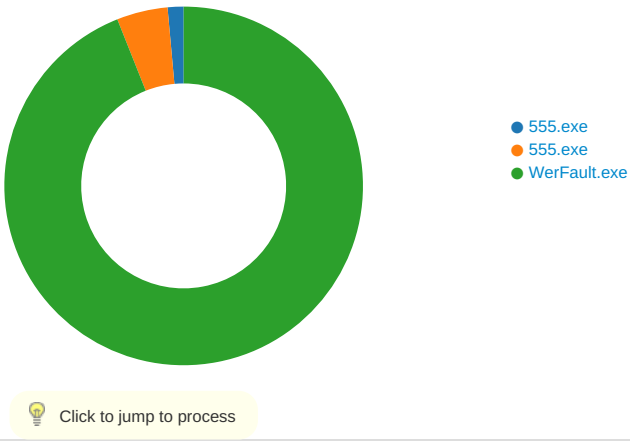
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 22, 2022 23:53:04.335752964 CET	192.168.2.4	8.8.8.8	0x1447	Standard query (0)	dersed.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 22, 2022 23:53:04.095592022 CET	8.8.8.8	192.168.2.4	0x8694	Name error (3)	dersed.com	none	none	A (IP address)	IN (0x0001)
Mar 22, 2022 23:53:04.136682034 CET	8.8.8.8	192.168.2.4	0xeb1c	Name error (3)	dersed.com	none	none	A (IP address)	IN (0x0001)
Mar 22, 2022 23:53:04.171823978 CET	8.8.8.8	192.168.2.4	0x99f3	Name error (3)	dersed.com	none	none	A (IP address)	IN (0x0001)
Mar 22, 2022 23:53:04.240736008 CET	8.8.8.8	192.168.2.4	0x774b	Name error (3)	dersed.com	none	none	A (IP address)	IN (0x0001)
Mar 22, 2022 23:53:04.281152964 CET	8.8.8.8	192.168.2.4	0x764c	Name error (3)	dersed.com	none	none	A (IP address)	IN (0x0001)
Mar 22, 2022 23:53:04.324481010 CET	8.8.8.8	192.168.2.4	0x2f6	Name error (3)	dersed.com	none	none	A (IP address)	IN (0x0001)
Mar 22, 2022 23:53:04.354562044 CET	8.8.8.8	192.168.2.4	0x1447	Name error (3)	dersed.com	none	none	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: 555.exe PID: 6192, Parent PID: 2920

General

Target ID:	0
Start time:	23:52:41
Start date:	22/03/2022
Path:	C:\Users\user\Desktop\555.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\555.exe"
Imagebase:	0x400000
File size:	1304576 bytes
MD5 hash:	ED37EBBE1746DD0D566C8C4769655E0B
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Oski_1, Description: Yara detected Oski Stealer, Source: 00000000.00000002.292388271.00000000048A5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000002.292388271.00000000048A5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski_1, Description: Yara detected Oski Stealer, Source: 00000000.00000002.291455838.00000000047B2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000002.291455838.00000000047B2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski_1, Description: Yara detected Oski Stealer, Source: 00000000.00000002.292903464.0000000004B5B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000000.00000002.292903464.0000000004B5B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D601.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40D13A	GetTempFileNameA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	41	75 6e 6b 6e 6f 77 6e	unknown	success or wait	80	42C1DD	WriteFile
unknown	unknown	0			invalid handle	1	4098CA	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
unknown	unknown	128	object type mismatch	1	408E8A	ReadFile
unknown	unknown	10	object type mismatch	1	408EB9	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: 555.exe PID: **6444**, Parent PID: **6192**

General

Target ID:	3
Start time:	23:52:59
Start date:	22/03/2022
Path:	C:\Users\user\Desktop\555.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\555.exe
Imagebase:	0x400000
File size:	1304576 bytes
MD5 hash:	ED37EBBE1746DD0D566C8C4769655E0B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Oski_1, Description: Yara detected Oski Stealer, Source: 00000003.00000000.294887526.0000000000474000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000003.00000000.294887526.0000000000474000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski_1, Description: Yara detected Oski Stealer, Source: 00000003.00000000.296551776.0000000000474000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000003.00000000.296551776.0000000000474000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski_1, Description: Yara detected Oski Stealer, Source: 00000003.00000002.317352104.0000000000474000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000003.00000002.317352104.0000000000474000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski_1, Description: Yara detected Oski Stealer, Source: 00000003.00000000.288286831.0000000000400000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000003.00000000.288286831.0000000000400000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Vidar, Description: Vidar Payload, Source: 00000003.00000000.288286831.0000000000400000.00000004.00000001.01000000.00000003.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\9ZWAQOQORWMXBQY6GLP6CSUUJ	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	406658	CreateDirectoryA
C:\ProgramData\9ZWAQOQORWMXBQY6GLP6CSUUJ\files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	406694	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409E52	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409E52	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409E52	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409E52	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409E52	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409E52	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409E52	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409E52	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409E52	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409E52	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409E52	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409E52	HttpSendRequestA
C:\ProgramData\9ZWAQOQORWMXBQY6GLP6CSUUJ\files\passwords.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	46CB49	CreateFileA
C:\ProgramData\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	413A9E	CreateDirectoryA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **6864**, Parent PID: **6444**

General

Target ID:	11
Start time:	23:53:07
Start date:	22/03/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6444 -s 1228
Imagebase:	0xb60000
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	6DFE1717	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4E21.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4E21.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_555.exe_73a2317c9b18c06fb4572ea77cd525ee3f28dbd_69550887_1ab655c1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_555.exe_73a2317c9b18c06fb4572ea77cd525ee3f28dbd_69550887_1ab655c1\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4E21.tmp	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4E21.tmp.xml	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER391B.tmp.csv	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER393B.tmp.txt	success or wait	1	6DFD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 57 53 3a 62 fd 05 12 00 00 00 00 00	MDMP WS:b	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	8224	6	00 00 00 00 00 00		success or wait	1	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.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 20 20 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 2c 19 00 00 4b 53 3a 62 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 0d 00 00 00 00 00 00 00 01 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UB GenuineIntelWT,KS:b0W . Europe Standard TimeW. Europe Daylight Time	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	9666	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 0f 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 5e fd fd 18 fd 19 00 fd 1d 41 00 23 00 00 00 46 02 01 00 30 fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++^A#F0+	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	1620	168	30 19 00 00 00 00 00 00 1d 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 1d 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 25 00 00	0A%	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	17542	20	2f 00 00 00 fd fd fd 00 00 00 00 00 3c 02 00 00 7a 47 00 00	/<zG	success or wait	47	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	18298	572	fd fd 3e 77 fd fd 3c 77 fd 00 00 00 fd fd fd fd 10 00 00 00 58 fd fd 00 24 fd fd 00 fd fd fd fd 40 fd 3c 77 40 fd 3c 77 fd fd fd fd 00 50 20 00 00 50 20 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd fd 00 00 00 fd fd fd fd 00 50 20 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 2f 7e 00 00 00 00 00 00 00 00 00 00 00 00 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 fd fd fd fd 0e 7e 00 00 00 00 00 00 00 00 00 fd 31 7e 00 00 fd 3f 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 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 00 fd fd fd 00 fd fd fd 00 fd fd fd 00 00 00 00 00 fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	>w<wX$@<w@<wP P P /~~1~?	success or wait	46	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	73782	256	fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 0c 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 1c 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 06 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 15 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 14 00 fd fd fd 01 03 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 03 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 14 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd cd 49 00 fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd	?w?w?w?w?w?w?w? w?w?w?wl?w?w?w	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	1788	4	0a 00 00 00		success or wait	10	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	10382	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 48 fd 19 00 fd fd 3e 77 23 00 00 00 06 02 00 00 fd fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++H>w#+	success or wait	10	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	2224	48	18 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 21 00 00 00 00 00 fd fd fd 02 00 00 00 00 3c 02 00 00 fd fd 00 00 fd 02 00 00 fd 41 00 00	!<A	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	2284	4	31 00 00 00	1	success or wait	49	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	8230	20	0e 00 00 00 35 00 35 00 35 00 2e 00 65 00 78 00 65 00 00 00	555.exe	success or wait	49	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	7472	752	00 00 fd 6d 00 00 00 00 00 40 01 00 fd 2a 01 00 fd 06 13 22 fd 25 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 70 fd 02 00 00 00 00 00 00 0f 03 00 00 00 00 fd 5d 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 29 fd 03 00 00 00 00 00 3b fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 1c 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 56 05 00 00 00 00	m@*"%BB? %@AZbp]);@V	success or wait	1	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	74038	18456	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3D28.tmp.dmp	32	108	03 00 00 00 fd 01 00 00 fd 06 00 00 04 00 00 00 fd 14 00 00 fd 08 00 00 05 00 00 00 fd 02 00 00 fd 44 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 78 2e 00 00 fd 3a 01 00 15 00 00 00 fd 01 00 00 fd 1d 00 00 16 00 00 00 fd 00 00 00 fd 1f 00 00	DT8Tx.:	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6444</Pid>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1002	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 35 00 35 00 35 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>555.exe</ImageName>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1062	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1066	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1070	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1160	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1164	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1168	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 39 00 36 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>12965</Uptime>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1212	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1216	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1220	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1302	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1306	2	09 00		success or wait	2	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1310	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1362	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1366	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1370	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1414	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1418	2	09 00		success or wait	3	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1424	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 30 00 39 00 34 00 35 00 33 00 33 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>109453312</PeakVirtualSize>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1512	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1516	2	09 00		success or wait	3	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1522	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 30 00 39 00 31 00 39 00 35 00 32 00 36 00 34 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>109195264</VirtualSize>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1594	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1598	2	09 00		success or wait	3	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1604	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 37 00 37 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>4775</PageFaultCount>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1678	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1682	2	09 00		success or wait	3	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1688	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 35 00 34 00 38 00 39 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>14548992</PeakWorkingSetSize>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1786	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1790	2	09 00		success or wait	3	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1796	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 35 00 34 00 38 00 39 00 39 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>14548992</WorkingSetSize>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1878	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1882	2	09 00		success or wait	3	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1888	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 32 00 30 00 31 00 39 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>201920</QuotaPeakPagedPoolUsage>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2002	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2006	2	09 00		success or wait	3	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2012	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 32 00 30 00 31 00 32 00 35 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>201256</QuotaPagedPoolUsage>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2110	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2114	2	09 00		success or wait	3	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2120	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 34 00 38 00 38 00 39 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>48896</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2244	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2248	2	09 00		success or wait	3	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2254	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 34 00 35 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>45504</QuotaNonPagedPoolUsage>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2362	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2366	2	09 00		success or wait	3	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2372	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 31 00 33 00 37 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4513792</PagefileUsage>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2448	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2452	2	09 00		success or wait	3	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2458	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 37 00 31 00 34 00 34 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>47114496</PeakPagefileUsage>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2550	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2554	2	09 00		success or wait	3	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2560	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 31 00 33 00 37 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4513792</PrivateUsage>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2632	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2636	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2640	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2686	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2690	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2694	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2724	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2728	2	09 00		success or wait	3	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2734	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2774	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2778	2	09 00		success or wait	4	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2786	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6192</Pid>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2816	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2820	2	09 00		success or wait	4	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2828	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 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>(unable to retrieve)</ImageName>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2914	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2918	2	09 00		success or wait	4	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2926	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3016	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3020	2	09 00		success or wait	4	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3028	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 30 00 39 00 30 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>30905</Uptime>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3072	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3076	2	09 00		success or wait	4	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3084	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3166	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3170	2	09 00		success or wait	4	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3178	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3230	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3234	2	09 00		success or wait	4	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3242	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3286	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3290	2	09 00		success or wait	5	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3300	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 34 00 32 00 37 00 34 00 39 00 36 00 39 00 36 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>142749696</PeakVirtualSize>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3388	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3392	2	09 00		success or wait	5	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3402	56	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 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>0</VirtualSize>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3472	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 35 00 36 00 33 00 31 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>15631</PageFaultCount>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3562	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 36 00 35 00 39 00 39 00 34 00 32 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>26599424</PeakWorkingSetSize>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3660	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3664	2	09 00		success or wait	5	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3674	76	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 32 00 30 00 34 00 38 00 30 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>20480</WorkingSetSize>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3750	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3754	2	09 00		success or wait	5	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3764	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 32 00 34 00 36 00 38 00 32 00 34 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>24682 4</QuotaPeakPagedPoolUsage>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3878	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3882	2	09 00		success or wait	5	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3892	88	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 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>0</QuotaPagedPoolUsage>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3980	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3984	2	09 00		success or wait	5	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3994	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21 448</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4118	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4122	2	09 00		success or wait	5	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4132	100	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 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>0</QuotaNonPagedPoolUsage>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4232	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4236	2	09 00		success or wait	5	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4246	72	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 31 00 34 00 34 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>61440</PagefileUsage>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4318	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4322	2	09 00		success or wait	5	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4332	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 32 00 35 00 34 00 30 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>14254080</PeakPagefileUsage>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4440	68	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 31 00 34 00 34 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>61440</PrivateUsage>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4508	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4512	2	09 00		success or wait	4	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4520	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4566	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4570	2	09 00		success or wait	3	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4576	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4618	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4622	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4626	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4664	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4706	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4710	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4712	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4758	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4820	4	0d 00 0a 00		success or wait	8	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4824	2	09 00		success or wait	16	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4828	64	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 35 00 35 00 35 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>555.exe</Parameter0>	success or wait	8	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5412	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5416	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5418	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5458	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5462	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5464	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5502	4	0d 00 0a 00		success or wait	6	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5506	2	09 00		success or wait	12	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5510	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6064	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6068	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6070	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6110	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6114	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6116	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6154	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6158	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6162	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6256	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6260	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6264	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 77 00 75 00 6f 00 63 00 61 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>wuocae, Inc.</SystemManufacturer>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6370	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6374	2	09 00		success or wait	2	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6378	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 77 00 75 00 6f 00 63 00 61 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>wuocae7,1</SystemProductName>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6474	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6478	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6482	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6602	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6606	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6610	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 30 00 35 00 37 00 30 00 37 00 36 00 36 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>1605707661</OSInstallDate>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6692	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6696	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6700	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6802	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6806	2	09 00		success or wait	2	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6810	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6880	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6884	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6886	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6926	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6930	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6932	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6966	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6970	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6974	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7070	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7074	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7076	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7112	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7116	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7118	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7142	4	0d 00 0a 00		success or wait	3	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7146	2	09 00		success or wait	6	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7150	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7408	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7412	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7414	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7440	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7444	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7446	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 33 00 2d 00 32 00 32 00 54 00 32 00 32 00 3a 00 35 00 33 00 3a 00 31 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-03-22T22:53:12Z">	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7546	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7550	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7554	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 34 00 34 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 35 00 32 00 30 00 33 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 35 00 32 00 30 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="405" PID="6444" UptimeMS="5203" TimeSinceCreationMS="5203" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7816	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7820	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7824	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	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7844	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7848	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7850	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7888	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7892	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7894	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7932	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7936	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7940	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 66 00 62 00 31 00 34 00 66 00 35 00 62 00 2d 00 38 00 32 00 38 00 30 00 2d 00 34 00 35 00 61 00 65 00 2d 00 62 00 65 00 65 00 39 00 2d 00 37 00 35 00 66 00 61 00 64 00 34 00 62 00 37 00 39 00 36 00 34 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>afb14f5b-8280-45ae-bee9-75fad4b7964f</Guid>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8038	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8042	2	09 00		success or wait	2	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8046	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 33 00 2d 00 32 00 32 00 54 00 32 00 32 00 3a 00 35 00 33 00 3a 00 31 00 32 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>2022-03-22T22:53:12Z</CreationTime>	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8144	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8148	2	09 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8150	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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8190	4	0d 00 0a 00		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8194	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	6DFD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4E21.tmp.xml	0	4522	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_555.exe_73a2317c9b18c06fb4572ea77cd525ee3f28dbd_69550887_1ab655c1\Report.wer	0	2	fd fd		success or wait	1	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_555.exe_73a2317c9b18c06fb4572ea77cd525ee3f28dbd_69550887_1ab655c1\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	6DFD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_555.exe_73a2317c9b18c06fb4572ea77cd525ee3f28dbd_69550887_1ab655c1\Report.wer	11884	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 30 00 31 00 34 00 33 00 32 00 32 00 31 00 38 00 37 00	MetadataHash=1014322187	success or wait	1	6DFD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	success or wait	1	6DFF36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6DFF1FB2	RegCreateKeyExW
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DFD43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	ProgramId	unicode	00065df13d417be7efd1d6509bfe9474853900000904	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	FileId	unicode	00000a559ebf6ab1cdf292c79aac5ac20c236d975eb7	success or wait	1	6DFF36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	LowerCaseLongPath	unicode	c:\users\user\desktop\555.exe	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	LongPathHash	unicode	555.exe|3b679044	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	Name	unicode	555.exe	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	Publisher	unicode	bitdefender llc	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	Version	unicode		success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	BinFileVersion	unicode	8.2.5.127	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	BinaryType	unicode	pe32_i386	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	ProductName	unicode	cnnmgrestablishcnnectin283715	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	ProductVersion	unicode	8.2.5.127	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	LinkDate	unicode	09/05/2019 12:37:08	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	BinProductVersion	unicode	8.2.5.127	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	Size	B	00 E8 13 00 00 00 00 00	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	Language	dword	1033	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	IsPeFile	dword	1	success or wait	1	6DFF36BF	unknown
\REGISTRY\A\{40ba1780-48b2-23c2-f33b-4b3db04d953e}\Root\InventoryApplicationFile\555.exe|3b679044	IsOsComponent	dword	0	success or wait	1	6DFF36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	1D 00 00 C0 00 00 00 00 00 00 00 00 FC 1D 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6DFF1FE8	RegSetValueExW

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

Disassembly

No disassembly