ID: 594633
Sample Name: 555.exe
Cookbook: default.jbs
Time: 00:01:37
Date: 23/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

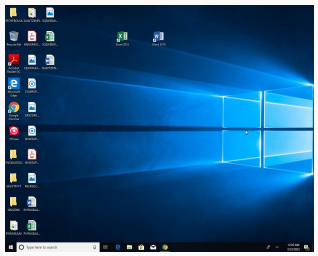
Windows Analysis Report

555.exe

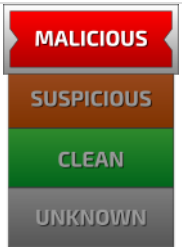
Overview

General Information

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



Detection



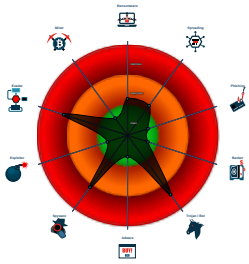
Oski Stealer Vidar

Score:	88
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
- 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
- Contains functionality to check if a d…

Classification



Process Tree

- **System is w10x64**
- 555.exe (PID: 6568 cmdline: "C:\Users\user\Desktop\555.exe" MD5: ED37EBBE1746DD0D566C8C4769655E0B)
  - 555.exe (PID: 6872 cmdline: C:\Users\user\Desktop\555.exe MD5: ED37EBBE1746DD0D566C8C4769655E0B)
    - WerFault.exe (PID: 5256 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6872 -s 1180 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.294243127.0000000000474000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_Oski_1	Yara detected Oski Stealer	Joe Security	
00000004.00000002.294243127.0000000000474000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000004.00000000.282266070.0000000000474000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_Oski_1	Yara detected Oski Stealer	Joe Security	
00000004.00000000.282266070.0000000000474000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000004.00000000.271412453.0000000000400000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_Oski_1	Yara detected Oski Stealer	Joe Security	

Click to see the 14 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.555.exe.400000.4.raw.unpack	JoeSecurity_Oski_1	Yara detected Oski Stealer	Joe Security	
4.0.555.exe.400000.4.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
4.0.555.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
4.2.555.exe.400000.0.unpack	JoeSecurity_Oski_1	Yara detected Oski Stealer	Joe Security	
4.2.555.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

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

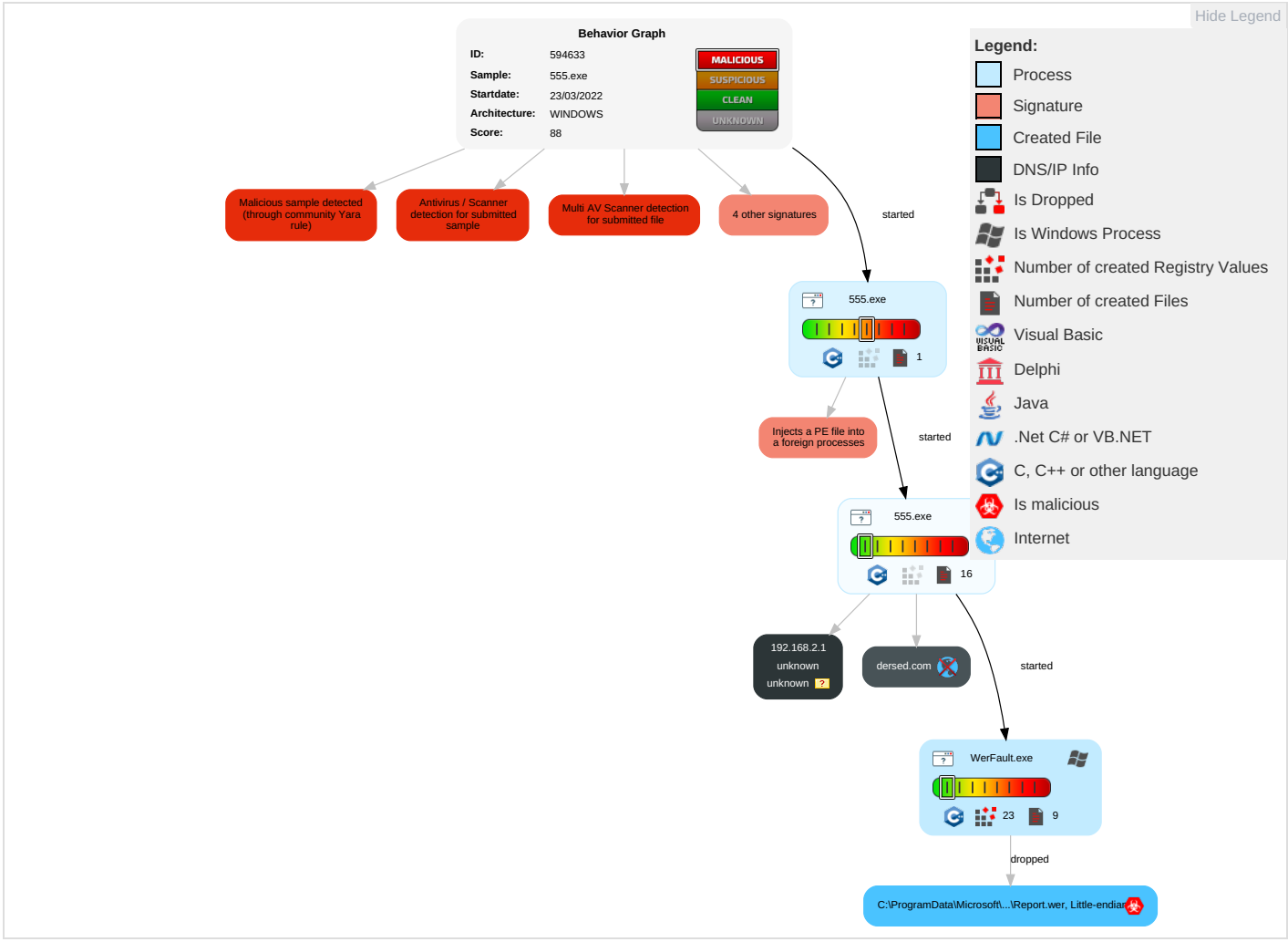
Yara detected Oski Stealer

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	3 Security Software Discovery	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	1 Virtualization/Sandbox Evasion	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	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 Application Window 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 Account 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 System Owner/User 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 Remote System 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	2 File and Directory 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 6 System Information Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

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
1.0.555.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1206114		Download File
4.2.555.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1210209		Download File
1.2.555.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1206114		Download File

Domains

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

URLs

No Antivirus matches

Domains and IPs

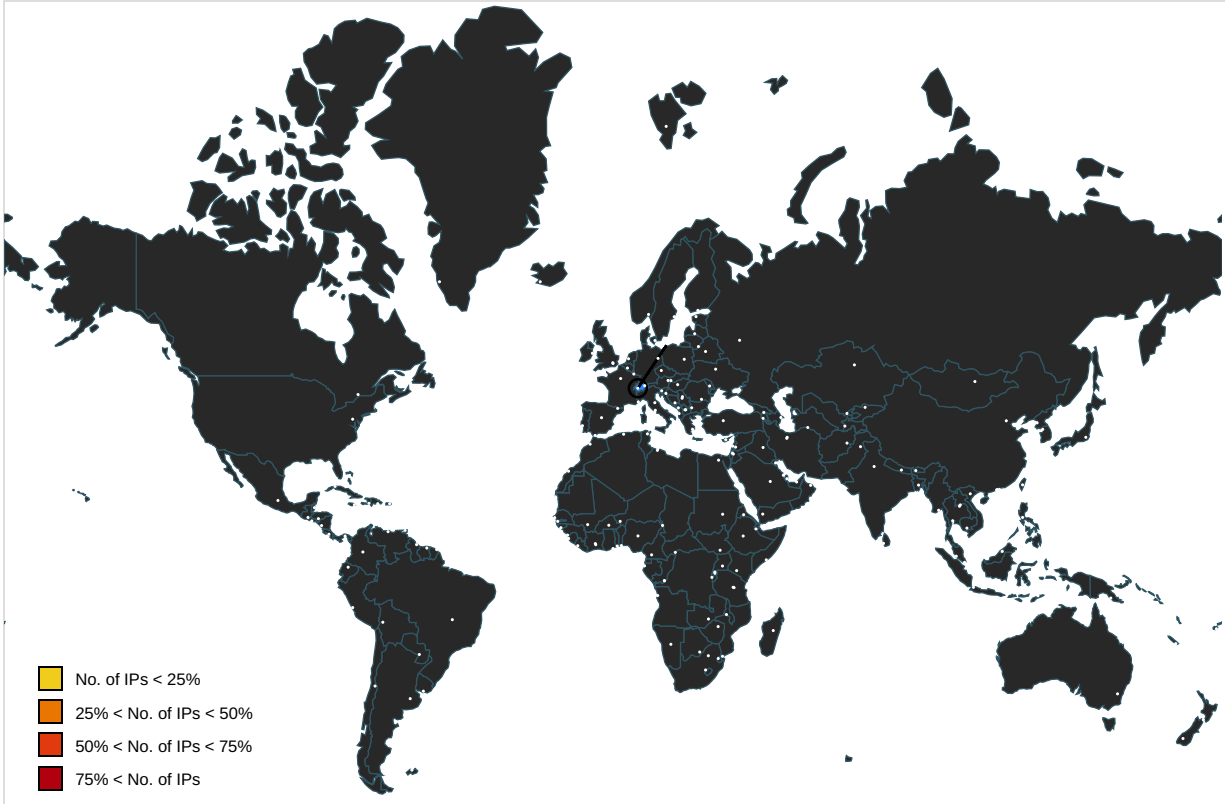
Contacted Domains

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://ip-api.com/line/	555.exe, 00000004.00000000.271412453.000 0000000400000.00000004.00000001.01000000 .00000003.sdmp	false		high

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 23:01:37 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 59s
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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.troj.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 • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, backgroundTaskHost.exe, UsoClient.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, UpdateNotificationMgr.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.42.65.92
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, arc.msn.com, ris.api.iris.microsoft.com, go.microsoft.com, onedsblobprdeus17.eastus.cloudapp.azure.com, login.live.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
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_555.exe_73a2317c9b18c06fb4572ea77cd525ee3f28dbd_69550887_14ead3ce\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):	0.9433130914041538
Encrypted:	false
SSDEEP:	192:d7HFk0lkNYHBUZMXIjAK3Yw/u7sjS274ItRA:ZHPlkSBUZMXIjL/u7sjX4ItR
MD5:	2E0957A2B87D7A5F4A2CC7B56AF4451B
SHA1:	615AC89639BD90D1072545A14B759DB05C0EA30C
SHA-256:	690C07D6C3E892C133D5AC774D70D6F30DB4CE2C230C43B861B0C6DA73A82940
SHA-512:	7FF6A9A5BBDA29F6B48F13DCCEC41CBE04FBEC43791A9617E33571C915CE5F1E49674E82306C94C9989442E99DF5A2857D149BE21918FA944DDF571BA162991D
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.=.1.3.2.9.2.4.9.2.5.7.8.3.2.5.0.1.2.0.....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.=.1.3.2.9.2.4.9.2.5.7.9.7.7.8.1.3.7.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.a.a.d.6.a.2.0.-.8.2.8.f.-.4.e.7.1.-.a.5.2.c.-.8.b.4.1.1.e.7.c.a.9.4.1.....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.5.0.b.1.6.d.2.-.6.5.3.f.-.4.1.b.1.-.8.9.c.4.-.8.2.e.4.f.d.9.9.5.4.9.4.....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.a.d.8.-.0.0.0.1.-.0.0.1.d.-.6.8.a.e.-.e.7.0.1.8.4.3.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\WERC93E.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Mar 23 07:02:58 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	86662
Entropy (8bit):	1.9961811068209203
Encrypted:	false
SSDEEP:	384:nYNwG+/CMBQ8LY8g7T9ZDEgqioxdzn9xJ/dLdY:djCIxLQmi8JVLd
MD5:	4136BC2E5A970E468649E0659FF9A15A
SHA1:	2308CE84A343683C735708B04F2E07DD8B90A679
SHA-256:	0D0AA7D55BFBFD15AB695894E71AA2C2028285843DD407AA49A1DF5B3CF81C16
SHA-512:	E9A9D7EE17158FD0355F93BC4678BFA5A3B493305027322FC9701199F43143D5E8E21FFFEAD0AC997E22A2883BC780897F3CCCB378A714C3E73BF92CFDD265E3
Malicious:	false
Reputation:	low

Preview:	MDMP..... .....".:b.....A.....T.....8.....T.....-...$.....l.....X.....U.....B.....GenuineIntelW.....T.....:b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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):	8230
Entropy (8bit):	3.6876573021210373
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNinI6IYqQ56Y/Q6JgmfhhSiCpra89bDOsfy3hm:RrlsNiI6IYj6YY6JgmfnSJDNfys
MD5:	897C3D138566EA49E505D64EFBC0F18A
SHA1:	DBC9F68811F3D3DF58E37987B6E31C0D41E1EF28
SHA-256:	F3967E703A0C7FCD8943EF2E17C771B8E3230BEB9A22FA5125C78232DCF7B783
SHA-512:	917E8E7295B06C15B393CE6CFAE781B03FBF4361A05D07F7136CBB11DDE916764A6A6AF7EBA19A190C6B828777C181164FEED383DB50AE7EE410CC145CE154A0
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.>.6.8.7.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDC5.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):	4.421241641980804
Encrypted:	false
SSDEEP:	48:cvIwSD8zsIJgtWI96iXWgc8sqYji8fm8M4J61RFhlF+q8m08whHXSrhdd:uITfOEmgrsqYjJ6FFQ8wxSrhdd
MD5:	D1D78CF6F562E818D892B2D5DD3C5FED
SHA1:	AE92D9038A1B018F68D24C74F0805680F9E6B5BF
SHA-256:	F3267A9B41B2E5A4820260B280F43AC5C9E864BFF51A58EEF9725E4E0AFEDEAF
SHA-512:	29A26A2B27F2C0141954A861BADDF32D7FB6C8BD6315968A8083C66A4F9141951F76057B7E5A94D980FA89AA27E8C95AC6F491590B63307878AD6F4E06B1D909
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="1439533" />.. <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 00007F4BACBD9BB9h
jmp 00007F4BACBD116Eh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
test eax, eax
je 00007F4BACBD12F4h
sub eax, 08h
cmp dword ptr [eax], 0000DDDDh
jne 00007F4BACBD12E9h
push eax
call 00007F4BACBCF0A2h
pop ecx
pop ebp
ret
mov edi, edi
push ebp
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

Instruction
xor ebx, ebx
push esi
push edi
cmp edx, ebx
jle 00007F4BACBD1301h
mov eax, dword ptr [ebp+14h]
mov ecx, edx
dec ecx
cmp byte ptr [eax], bl
je 00007F4BACBD12EAh
inc eax
cmp ecx, ebx
jne 00007F4BACBD12D8h
or ecx, FFFFFFFFh
mov eax, edx
sub eax, ecx
dec eax
cmp eax, edx
jnl 00007F4BACBD12E3h
inc eax
mov dword ptr [ebp+18h], eax
mov dword ptr [ebp-08h], ebx
cmp dword ptr [ebp+24h], ebx
jne 00007F4BACBD12EDh
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 00007F4BACBD12E9h
xor eax, eax
jmp 00007F4BACBD1437h
jle 00007F4BACBD1325h
push FFFFFFE0h
xor edx, edx
pop eax
div edi
cmp eax, 02h
jc 00007F4BACBD1319h
lea eax, dword ptr [edi+edi+08h]
cmp eax, 00000400h
jnbe 00007F4BACBD12F5h
call 00007F4BACBD1394h

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
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

Name	RVA	Size	Type	Language	Country
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
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

Description	Data
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 23, 2022 00:02:55.275547028 CET	49873	53	192.168.2.3	8.8.8.8
Mar 23, 2022 00:02:55.296334982 CET	53	49873	8.8.8.8	192.168.2.3
Mar 23, 2022 00:02:55.325387001 CET	53802	53	192.168.2.3	8.8.8.8
Mar 23, 2022 00:02:55.345118999 CET	53	53802	8.8.8.8	192.168.2.3
Mar 23, 2022 00:02:55.354346037 CET	65266	53	192.168.2.3	8.8.8.8
Mar 23, 2022 00:02:55.374769926 CET	53	65266	8.8.8.8	192.168.2.3
Mar 23, 2022 00:02:55.399142981 CET	63332	53	192.168.2.3	8.8.8.8
Mar 23, 2022 00:02:55.419553995 CET	53	63332	8.8.8.8	192.168.2.3
Mar 23, 2022 00:02:55.427473068 CET	63548	53	192.168.2.3	8.8.8.8
Mar 23, 2022 00:02:55.449235916 CET	53	63548	8.8.8.8	192.168.2.3
Mar 23, 2022 00:02:55.456845999 CET	49327	53	192.168.2.3	8.8.8.8
Mar 23, 2022 00:02:55.476484060 CET	53	49327	8.8.8.8	192.168.2.3
Mar 23, 2022 00:02:55.486458063 CET	51391	53	192.168.2.3	8.8.8.8
Mar 23, 2022 00:02:55.508095026 CET	53	51391	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 23, 2022 00:02:55.275547028 CET	192.168.2.3	8.8.8.8	0x6a33	Standard query (0)	dersed.com	A (IP address)	IN (0x0001)
Mar 23, 2022 00:02:55.325387001 CET	192.168.2.3	8.8.8.8	0x7cc7	Standard query (0)	dersed.com	A (IP address)	IN (0x0001)
Mar 23, 2022 00:02:55.354346037 CET	192.168.2.3	8.8.8.8	0xa8b3	Standard query (0)	dersed.com	A (IP address)	IN (0x0001)
Mar 23, 2022 00:02:55.399142981 CET	192.168.2.3	8.8.8.8	0x87af	Standard query (0)	dersed.com	A (IP address)	IN (0x0001)
Mar 23, 2022 00:02:55.427473068 CET	192.168.2.3	8.8.8.8	0x4d42	Standard query (0)	dersed.com	A (IP address)	IN (0x0001)
Mar 23, 2022 00:02:55.456845999 CET	192.168.2.3	8.8.8.8	0x4146	Standard query (0)	dersed.com	A (IP address)	IN (0x0001)
Mar 23, 2022 00:02:55.486458063 CET	192.168.2.3	8.8.8.8	0x6dfc	Standard query (0)	dersed.com	A (IP address)	IN (0x0001)

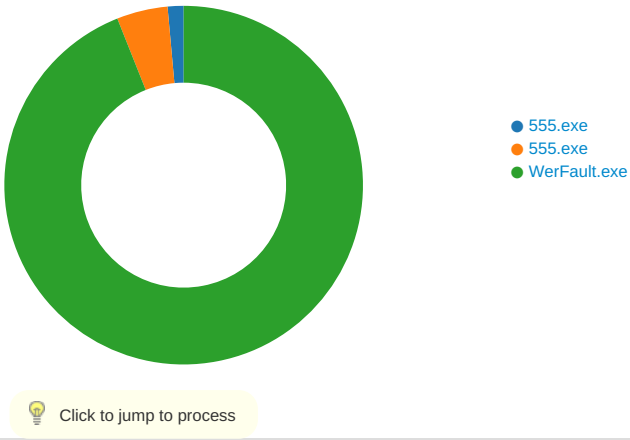
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 23, 2022 00:02:55.296334982 CET	8.8.8.8	192.168.2.3	0x6a33	Name error (3)	dersed.com	none	none	A (IP address)	IN (0x0001)
Mar 23, 2022 00:02:55.345118999 CET	8.8.8.8	192.168.2.3	0x7cc7	Name error (3)	dersed.com	none	none	A (IP address)	IN (0x0001)
Mar 23, 2022 00:02:55.374769926 CET	8.8.8.8	192.168.2.3	0xa8b3	Name error (3)	dersed.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 23, 2022 00:02:55.419553995 CET	8.8.8.8	192.168.2.3	0x87af	Name error (3)	dersed.com	none	none	A (IP address)	IN (0x0001)
Mar 23, 2022 00:02:55.449235916 CET	8.8.8.8	192.168.2.3	0x4d42	Name error (3)	dersed.com	none	none	A (IP address)	IN (0x0001)
Mar 23, 2022 00:02:55.476484060 CET	8.8.8.8	192.168.2.3	0x4146	Name error (3)	dersed.com	none	none	A (IP address)	IN (0x0001)
Mar 23, 2022 00:02:55.508095026 CET	8.8.8.8	192.168.2.3	0x6dfc	Name error (3)	dersed.com	none	none	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: 555.exe PID: **6568**, Parent PID: **240**

General

Target ID:	1
Start time:	00:02:36
Start date:	23/03/2022
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: 00000001.00000002.280513930.0000000004B63000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000002.280513930.0000000004B63000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski_1, Description: Yara detected Oski Stealer, Source: 00000001.00000002.280000448.00000000047CA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000002.280000448.00000000047CA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski_1, Description: Yara detected Oski Stealer, Source: 00000001.00000002.280450164.00000000048D8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000001.00000002.280450164.00000000048D8000.00000004.00000800.00020000.00000000.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\787F.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: **6872**, Parent PID: **6568**

General

Target ID:	4
Start time:	00:02:49
Start date:	23/03/2022
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: 00000004.00000002.294243127.0000000000474000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000004.00000002.294243127.0000000000474000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski_1, Description: Yara detected Oski Stealer, Source: 00000004.00000000.282266070.0000000000474000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000004.00000000.282266070.0000000000474000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski_1, Description: Yara detected Oski Stealer, Source: 00000004.00000000.271412453.0000000000400000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000004.00000000.271412453.0000000000400000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Vidar, Description: Vidar Payload, Source: 00000004.00000000.271412453.0000000000400000.00000004.00000001.01000000.00000003.sdmp, Author: kevoreilly • Rule: JoeSecurity_Oski_1, Description: Yara detected Oski Stealer, Source: 00000004.00000000.281204973.0000000000474000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000004.00000000.281204973.0000000000474000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\NZSXU0TPWFN29SVMNBQB4Z5K6	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\NZSXU0TPWFN29SVMNBQB4Z5K6\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
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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\NZSXU0TPWFN29SVMNBQB4Z5K6\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: **5256**, Parent PID: **6872**

General

Target ID:	7
Start time:	00:02:57
Start date:	23/03/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6872 -s 1180
Imagebase:	0x80000
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	6E341717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDC5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDC5.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E33497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_555.exe_73a2317c9b18c06fb4572ea77cd525ee3f28dbd_69550887_14ead3ce	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_555.exe_73a2317c9b18c06fb4572ea77cd525ee3f28dbd_69550887_14ead3ce\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E33497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDC5.tmp	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDC5.tmp.xml	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD77.tmp.csv	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD88.tmp.txt	success or wait	1	6E33497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 22 fd 3a 62 fd 05 12 00 00 00 00 00	MDMP ":b	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	8176	6	00 00 00 00 00 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.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 fd 1f 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 1a 00 00 19 fd 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 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT:b0Pacific Standard TimePacific Daylight Time	success or wait	1	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	9618	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 0f 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 06 52 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 fd fd fd fd	+S++RA#F0+	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	1620	168	fd 1a 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 fd 02 00 00 fd 25 00 00	A%	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	16778	20	2a 00 00 00 fd 07 57 00 00 00 00 00 04 00 00 00 2e 44 00 00	*W.D	success or wait	42	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	17454	4	fd fd fd 02		success or wait	41	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	68226	288	2c fd 4c 77 19 07 fd 75 fd 02 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 58 00 fd fd fd fd fd 58 00 24 00 00 00 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 00 00 00 00 00 00 00 00 fd fd fd 02 fd 1e fd 75 fd fd fd fd 00 00 00 00 68 fd fd 02 72 06 fd 75 fd 02 00 00 fd fd fd fd 00 00 00 00 fd fd fd 02 32 fd fd 6f fd 02 00 00 fd fd fd fd 00 fd fd 6f 00 fd fd 6f fd fd fd 02 fd fd 1b 76 fd fd 58 00 60 fd 1b 76 fd fd fd fd fd fd 02 fd 2e 4c 77 fd fd 58 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd 58 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd 02 00 00 00 00 fd fd fd 02 fd 17 4d 77 fd fd fd fd 00 00 00 00 fd fd fd	,LwuXX$uhru2ooovX`v.LwXXMw	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	1788	4	09 00 00 00		success or wait	9	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	10334	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 4c 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 fd fd fd fd	?+S++HLw#+	success or wait	9	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	2176	48	6c 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 20 00 00 00 00 00 fd fd fd 02 00 00 00 00 3c 02 00 00 06 fd 00 00 fd 02 00 00 fd 3e 00 00	l <>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	2236	4	31 00 00 00	1	success or wait	49	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	8182	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	7424	752	00 00 fd 6d 00 00 00 00 00 40 01 00 fd 2a 01 00 fd 06 13 22 74 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 00 fd 02 00 00 00 00 00 00 1a 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 d8 03 00 00 00 00 00 0f fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 1b 00 00 00 00 00 70 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6c 05 00 00 00 00	m@*"t%BB?%@AZbp@l	success or wait	1	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.tmp.dmp	68514	18148	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93E.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 41 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 2d 00 00 fd 24 01 00 15 00 00 00 fd 01 00 00 6c 1d 00 00 16 00 00 00 fd 00 00 00 58 1f 00 00	AT8T-$lX	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6872</Pid>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1062	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1066	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1160	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1164	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1168	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 35 00 32 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>9522</Uptime>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1210	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1214	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1218	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1300	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1304	2	09 00		success or wait	2	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1308	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1360	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1364	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1368	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1412	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1416	2	09 00		success or wait	3	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1422	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 38 00 30 00 33 00 36 00 30 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>108036096</PeakVirtualSize>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1510	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1514	2	09 00		success or wait	3	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1520	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 37 00 37 00 37 00 38 00 30 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>107778048</VirtualSize>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1592	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1596	2	09 00		success or wait	3	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1602	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 31 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>4711</PageFaultCount>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1676	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1680	2	09 00		success or wait	3	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1686	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 34 00 33 00 34 00 33 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>14434304</PeakWorkingSetSize>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1784	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1788	2	09 00		success or wait	3	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1794	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 34 00 34 00 33 00 34 00 33 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>14434304</WorkingSetSize>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1876	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1880	2	09 00		success or wait	3	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	1886	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 32 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 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>201248</QuotaPeakPagedPoolUsage>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2000	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2004	2	09 00		success or wait	3	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2010	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 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>201032</QuotaPagedPoolUsage>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2108	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2112	2	09 00		success or wait	3	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2118	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 37 00 39 00 34 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 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>47944</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2242	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2246	2	09 00		success or wait	3	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2252	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 34 00 36 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>44648</QuotaNonPagedPoolUsage>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2360	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2364	2	09 00		success or wait	3	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2370	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 34 00 31 00 39 00 35 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4419584</PagefileUsage>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2446	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2450	2	09 00		success or wait	3	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2456	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 36 00 31 00 36 00 31 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>4616192</PeakPagefileUsage>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2548	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2552	2	09 00		success or wait	3	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2558	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 34 00 31 00 39 00 35 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4419584</PrivateUsage>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2630	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2634	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2638	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2684	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2688	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2692	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2722	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2726	2	09 00		success or wait	3	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2732	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2772	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2776	2	09 00		success or wait	4	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2784	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6568</Pid>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2814	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2818	2	09 00		success or wait	4	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2826	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2912	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2916	2	09 00		success or wait	4	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	2924	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3014	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3018	2	09 00		success or wait	4	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3026	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 32 00 34 00 37 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>22476</Uptime>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3070	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3074	2	09 00		success or wait	4	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3082	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3176	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3240	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3298	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 35 00 39 00 32 00 38 00 31 00 39 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>145928192</PeakVirtualSize>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3386	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3390	2	09 00		success or wait	5	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3400	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3456	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3460	2	09 00		success or wait	5	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3470	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 37 00 31 00 34 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>15714</PageFaultCount>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3546	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3550	2	09 00		success or wait	5	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3560	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 38 00 38 00 32 00 30 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>26882048</PeakWorkingSetSize>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3672	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3762	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 35 00 32 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>252952</QuotaPeakPagedPoolUsage>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3876	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3880	2	09 00		success or wait	5	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3890	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3978	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3982	2	09 00		success or wait	5	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	3992	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 38 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>21848</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4116	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4120	2	09 00		success or wait	5	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4130	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4244	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4316	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4320	2	09 00		success or wait	5	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4330	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 33 00 31 00 39 00 36 00 31 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>14319616</PeakPagefileUsage>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4424	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4428	2	09 00		success or wait	5	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4438	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4506	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4510	2	09 00		success or wait	4	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4518	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4564	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4568	2	09 00		success or wait	3	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4574	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4624	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4656	4	0d 00 0a 00		success or wait	1	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4660	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4662	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4710	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4748	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4752	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4756	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4818	4	0d 00 0a 00		success or wait	8	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4822	2	09 00		success or wait	16	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	4826	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	5410	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	5414	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	5416	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	5456	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	5460	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	5462	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	5500	4	0d 00 0a 00		success or wait	6	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	5504	2	09 00		success or wait	12	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	5508	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6062	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6066	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6068	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6108	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6112	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6114	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6152	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6156	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6160	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6254	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6258	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6262	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 67 00 74 00 64 00 77 00 6e 00 6e 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>gtdwnn, Inc.</SystemManufacturer>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6368	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6372	2	09 00		success or wait	2	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6376	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 67 00 74 00 64 00 77 00 6e 00 6e 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>gtdwnn7,1</SystemProductName>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6472	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6476	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6480	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6600	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6604	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6608	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 31 00 36 00 36 00 30 00 37 00 34 00 38 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>1601660748</OSInstallDate>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6690	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6694	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6698	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6800	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6804	2	09 00		success or wait	2	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6808	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6876	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6880	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6882	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6922	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6926	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6928	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6962	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6966	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	6970	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7066	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7070	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7072	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7108	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7112	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7114	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7138	4	0d 00 0a 00		success or wait	3	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7142	2	09 00		success or wait	6	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7146	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7404	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7408	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7410	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7436	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7440	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7442	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 33 00 54 00 30 00 37 00 3a 00 30 00 32 00 3a 00 35 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-03-23T07:02:59Z">	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7542	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7546	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7550	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 39 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 38 00 37 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 35 00 39 00 32 00 31 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 39 00 32 00 31 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="397" PID="6872" UptimeMS="5921" TimeSinceCreationMS="5921" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7812	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7816	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7820	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	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7840	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7844	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7846	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7884	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7888	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7890	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7928	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7932	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	7936	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 61 00 61 00 64 00 36 00 61 00 32 00 30 00 2d 00 38 00 32 00 38 00 66 00 2d 00 34 00 65 00 37 00 31 00 2d 00 61 00 35 00 32 00 63 00 2d 00 38 00 62 00 34 00 31 00 31 00 65 00 37 00 63 00 61 00 39 00 34 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>daad6a20-828f-4e71-a52c-8b411e7ca941</Guid>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	8034	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	8038	2	09 00		success or wait	2	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	8042	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 33 00 54 00 30 00 37 00 3a 00 30 00 32 00 3a 00 35 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-03-23T07:02:59Z</CreationTime>	success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	8140	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	8144	2	09 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	8146	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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	8186	4	0d 00 0a 00		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC5C.tmp.WERInternalMetadata.xml	8190	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	6E33497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDC5.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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_555.exe_73a2317c9b18c06fb4572ea77cd525ee3f28dbd_69550887_14ead3ce\Report.wer	0	2	fd fd		success or wait	1	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_555.exe_73a2317c9b18c06fb4572ea77cd525ee3f28dbd_69550887_14ead3ce\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	6E33497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_555.exe_73a2317c9b18c06fb4572ea77cd525ee3f28dbd_69550887_14ead3ce\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 32 00 38 00 31 00 36 00 32 00 39 00 38 00 32 00 35 00	MetadataHash=1281629825	success or wait	1	6E33497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	success or wait	1	6E3536BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6E351FB2	RegCreateKeyExW
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E3343D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	ProgramId	unicode	00065df13d417be7efd1d6509bfe9474853900000904	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	FileId	unicode	00000a559ebf6ab1cdf292c79aac5ac20c236d975eb7	success or wait	1	6E3536BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	LowerCaseLongPath	unicode	c:\users\user\desktop\555.exe	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	LongPathHash	unicode	555.exe|72eb515	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	Name	unicode	555.exe	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	Publisher	unicode	bitdefender llc	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	Version	unicode		success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	BinFileVersion	unicode	8.2.5.127	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	BinaryType	unicode	pe32_i386	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	ProductName	unicode	cnnmgrestablishcnnectin283715	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	ProductVersion	unicode	8.2.5.127	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	LinkDate	unicode	09/05/2019 12:37:08	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	BinProductVersion	unicode	8.2.5.127	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	Size	B	00 E8 13 00 00 00 00 00	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	Language	dword	1033	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	IsPeFile	dword	1	success or wait	1	6E3536BF	unknown
\REGISTRY\A\{672f463c-baaf-fd5b-54a9-e7320b9c4ec4}\Root\InventoryApplicationFile\555.exe|72eb515	IsOsComponent	dword	0	success or wait	1	6E3536BF	unknown
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	6E351FE8	RegSetValueExW

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

Disassembly

No disassembly