ID: 798336
Sample Name: PhviZrlpkW.exe
Cookbook: default.jbs
Time: 23:16:11
Date: 03/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2023

Copyright Joe Security LLC 2023

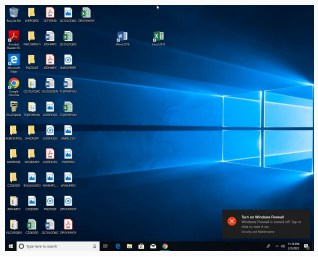
Windows Analysis Report

PhviZrlpkW.exe

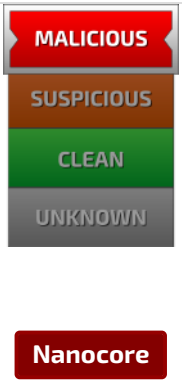
Overview

General Information

Sample Name:	PhviZrlpkW.exe
Analysis ID:	798336
MD5:	565044691fedb..
SHA1:	d92f48359c385..
SHA256:	3a1c1eabfbe52..
Tags:	exe NanoCore RAT
Infos:	



Detection



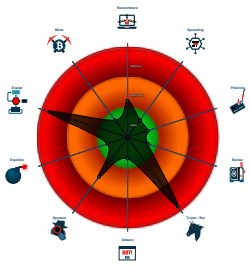
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Detected unpacking (creates a PE f…
- Snort IDS alert for network traffic
- Maps a DLL or memory area into an…
- .NET source code contains potentia…
- Found evasive API chain (may stop…

Classification



Process Tree

- **System is w10x64**
- PhviZrlpkW.exe (PID: 4624 cmdline: C:\Users\user\Desktop\PhviZrlpkW.exe MD5: 565044691FEDB39980CB814DC26F9EBD)
  - tchnhwrvi.exe (PID: 2120 cmdline: "C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe" C:\Users\user\AppData\Local\Temp\lcrizgqjcc.mo MD5: 64F982758878F6A97ED4B3D99CFBD371)
    - tchnhwrvi.exe (PID: 1312 cmdline: C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe MD5: 64F982758878F6A97ED4B3D99CFBD371)
  - edpm.exe (PID: 2468 cmdline: "C:\Users\user\AppData\Roaming\ovawcpafrwk\edpm.exe" "C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe" C:\Users\user\AppData\Loca MD5: 64F982758878F6A97ED4B3D99CFBD371)
    - WerFault.exe (PID: 1256 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2468 -s 656 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - edpm.exe (PID: 5104 cmdline: "C:\Users\user\AppData\Roaming\ovawcpafrwk\edpm.exe" "C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe" C:\Users\user\AppData\Loca MD5: 64F982758878F6A97ED4B3D99CFBD371)
    - WerFault.exe (PID: 3692 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5104 -s 632 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: NanoCore

Copyright Joe Security LLC 2023

```
{
  "Version": "1.2.2.0",
  "Mutex": "fc2f5233-89c0-4cab-99aa-8d389dd5",
  "Domain1": "thesopranos.duckdns.org",
  "Domain2": "thesopranos.duckdns.org",
  "Port": 1365,
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.567185811.0000000004E2C000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000002.00000002.567185811.0000000004E2C000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe91:$a: NanoCore • 0xeea:$a: NanoCore • 0xf27:$a: NanoCore • 0xfa0:$a: NanoCore • 0x1464b:$a: NanoCore • 0x14660:$a: NanoCore • 0x14695:$a: NanoCore • 0x222aa:$a: NanoCore • 0x222cf:$a: NanoCore • 0x22328:$a: NanoCore • 0x324c5:$a: NanoCore • 0x324eb:$a: NanoCore • 0x32547:$a: NanoCore • 0x3f39c:$a: NanoCore • 0x3f3f5:$a: NanoCore • 0x3f428:$a: NanoCore • 0x3f654:$a: NanoCore • 0x3f6d0:$a: NanoCore • 0x3fce9:$a: NanoCore • 0x3fe32:$a: NanoCore • 0x40306:$a: NanoCore
00000002.00000002.567185811.0000000004E2C000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xf27:$a1: NanoCore.ClientPluginHost • 0x14695:$a1: NanoCore.ClientPluginHost • 0x222cf:$a1: NanoCore.ClientPluginHost • 0x324eb:$a1: NanoCore.ClientPluginHost • 0x3f654:$a1: NanoCore.ClientPluginHost • 0x45ba2:$a1: NanoCore.ClientPluginHost • 0x4bb73:$a1: NanoCore.ClientPluginHost • 0x555df:$a1: NanoCore.ClientPluginHost • 0x5fa0a:$a1: NanoCore.ClientPluginHost • 0x6a9e7:$a1: NanoCore.ClientPluginHost • 0xeea:$a2: NanoCore.ClientPlugin • 0x14660:$a2: NanoCore.ClientPlugin • 0x222aa:$a2: NanoCore.ClientPlugin • 0x324c5:$a2: NanoCore.ClientPlugin • 0x3f6d0:$a2: NanoCore.ClientPlugin • 0x45c1c:$a2: NanoCore.ClientPlugin • 0x4bbbd:$a2: NanoCore.ClientPlugin • 0x556c9:$a2: NanoCore.ClientPlugin • 0x5faaa:$a2: NanoCore.ClientPlugin • 0x6a9be:$a2: NanoCore.ClientPlugin • 0x12be:$b1: get_BuilderSettings

Copyright Joe Security LLC 2023

Source	Rule	Description	Author	Strings
00000002.00000002.564994074.0000000001587000.00000004.00000020.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x26455:$x1: NanoCore.ClientPluginHost • 0x26492:$x2: IClientNetworkHost • 0x29fc5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000002.00000002.564994074.0000000001587000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 100 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.tchnhwrvi.exe.4f14bbe.11.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x170b:$x1: NanoCore.ClientPluginHost • 0x1725:$x2: IClientNetworkHost
2.2.tchnhwrvi.exe.4f14bbe.11.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x170b:$x2: NanoCore.ClientPluginHost • 0x34b6:$s4: PipeCreated • 0x16f8:$s5: IClientLoggingHost
2.2.tchnhwrvi.exe.4f14bbe.11.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x16e2:$x2: NanoCore.ClientPlugin • 0x170b:$x3: NanoCore.ClientPluginHost • 0x16d3:$i3: IClientNetwork • 0x16f8:$i6: IClientLoggingHost • 0x1725:$i7: IClientNetworkHost • 0x154e:$s1: ClientPlugin • 0x16eb:$s1: ClientPlugin
2.2.tchnhwrvi.exe.4f14bbe.11.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x170b:$a1: NanoCore.ClientPluginHost • 0x16e2:$a2: NanoCore.ClientPlugin • 0x3a54:$b7: LogClientException • 0x16f8:$b9: IClientLoggingHost
2.2.tchnhwrvi.exe.73f0000.33.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost
Click to see the 336 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138 −

Timestamp:	192.168.2.4193.31.30.1384972613652816766 02/03/23-23:19:06.285273
SID:	2816766
Source Port:	49726
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2023

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.1384971313652816766 02/03/23-23:17:46.673206
SID:	2816766
Source Port:	49713
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.1384971813652816766 02/03/23-23:18:21.376630
SID:	2816766
Source Port:	49718
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.1384972113652816766 02/03/23-23:18:33.469715
SID:	2816766
Source Port:	49721
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.1384971613652816766 02/03/23-23:18:07.532553
SID:	2816766
Source Port:	49716
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.1384971413652816766 02/03/23-23:17:53.669627
SID:	2816766
Source Port:	49714
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.1384972313652816766 02/03/23-23:18:47.034655
SID:	2816766
Source Port:	49723
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 193.31.30.138 - Destination IP: 192.168.2.4	
Timestamp:	193.31.30.138192.168.2.41365497022810290 02/03/23-23:17:30.731633
SID:	2810290
Source Port:	1365
Destination Port:	49702
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.1384972513652816718 02/03/23-23:18:58.945928
SID:	2816718
Source Port:	49725

Copyright Joe Security LLC 2023

Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.138497021365281676 6 02/03/23-23:17:32.574212
SID:	2816766
Source Port:	49702
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.138497171365281676 6 02/03/23-23:18:13.577404
SID:	2816766
Source Port:	49717
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.138497141365281671 8 02/03/23-23:17:52.672539
SID:	2816718
Source Port:	49714
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.138497121365281676 6 02/03/23-23:17:40.364031
SID:	2816766
Source Port:	49712
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.138497221365281676 6 02/03/23-23:18:41.032521
SID:	2816766
Source Port:	49722
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.138497251365281676 6 02/03/23-23:18:59.896530
SID:	2816766
Source Port:	49725
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.138496931365281676 6 02/03/23-23:17:25.471865
SID:	2816766
Source Port:	49693
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.1384971513652816766 02/03/23-23:18:01.525116
SID:	2816766
Source Port:	49715
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.1384969113652816766 02/03/23-23:17:14.041382
SID:	2816766
Source Port:	49691
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.1384972013652816766 02/03/23-23:18:27.458779
SID:	2816766
Source Port:	49720
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 193.31.30.138	
Timestamp:	192.168.2.4193.31.30.1384972413652816766 02/03/23-23:18:53.018271
SID:	2816766
Source Port:	49724
Destination Port:	1365
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dropped file
- Yara detected Nanocore RAT

Compliance

- Detected unpacking (creates a PE file in dynamic memory)

Networking

- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

E-Banking Fraud

- Yara detected Nanocore RAT

Copyright Joe Security LLC 2023

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (creates a PE file in dynamic memory)

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

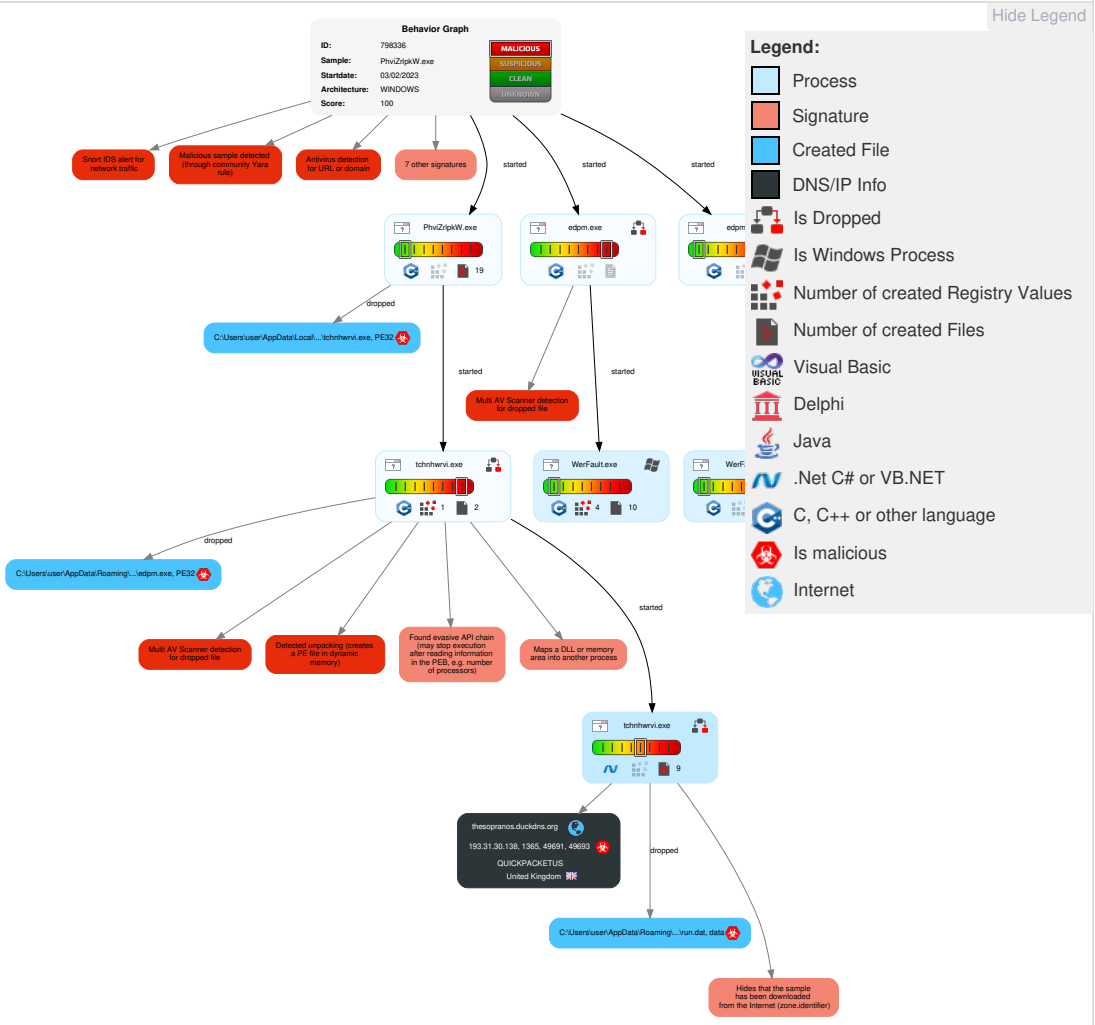
Yara detected Nanocore RAT

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 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	1 Disable or Modify Tools	2 1 Input Capture	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 2 Native API	Boot or Logon Initialization Scripts	1 1 2 Process Injection	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Command and Scripting Interpreter	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	2 Obfuscated Files or Information	Security Account Manager	2 6 System Information Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 1 Software Packing	NTDS	1 4 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 2 Process Injection	Proc Filesystem	1 Remote System 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)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

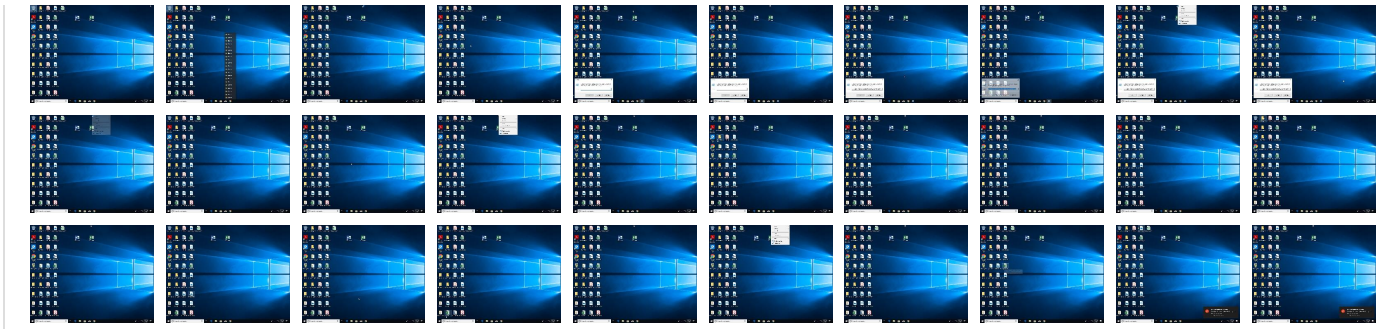
Behavior Graph



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
PhviZrlpkW.exe	58%	ReversingLabs	Win32.Trojan.Nsisx	
PhviZrlpkW.exe	53%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe	65%	ReversingLabs	Win32.Trojan.NSISInject	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe	52%	Virustotal		Browse
C:\Users\user\AppData\Roaming\ovawcpafrwk\edpm.exe	65%	ReversingLabs	Win32.Trojan.NSISInject	
C:\Users\user\AppData\Roaming\ovawcpafrwk\edpm.exe	52%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.tchnhwrvi.exe.aa0000.1.unpack	100%	Avira	HEUR/AGEN.1215480		Download File
2.2.tchnhwrvi.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.PhviZrlpkW.exe.28a8998.1.unpack	100%	Avira	HEUR/AGEN.1215480		Download File
2.2.tchnhwrvi.exe.5df0000.31.unpack	100%	Avira	TR/NanoCore.fadte		Download File
2.2.tchnhwrvi.exe.441b408.27.unpack	100%	Avira	TR/NanoCore.fadte		Download File
2.2.tchnhwrvi.exe.3330000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
thesopranos.duckdns.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
thesopranos.duckdns.org	1%	Virustotal		Browse
thesopranos.duckdns.org	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
thesopranos.duckdns.org	193.31.30.138	true	true	• 1%, Virustotal, Browse	unknown

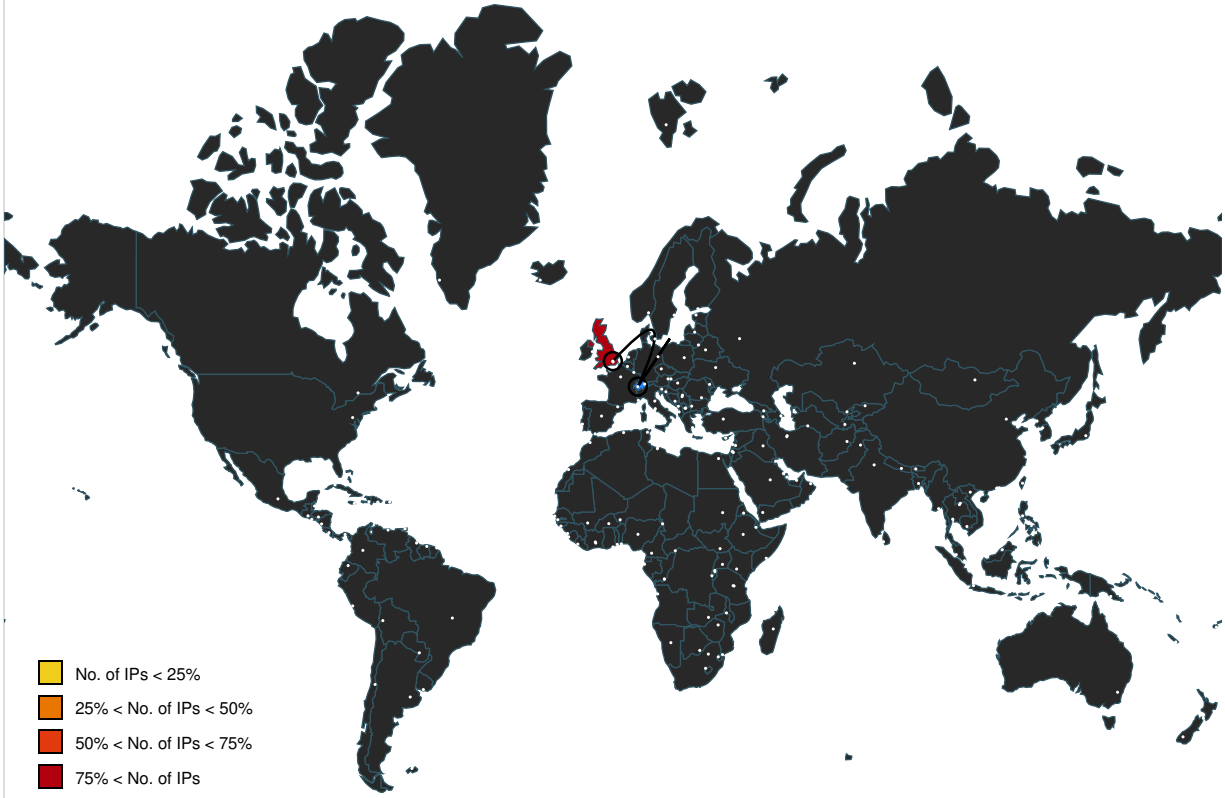
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
thesopranos.duckdns.org	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	PhviZrlpkW.exe	false		high
http://google.com	tchnhwrvi.exe, 00000002.00000002.567185811.0000000004E2C000.00000004.00000800.00020000.00000000.sdmp, tchnhwrvi.exe, 00000002.00000002.567185811.0000000004C83000.00000004.00000800.00020000.00000000.sdmp, tchnhwrvi.exe, 00000002.00000002.566066458.00000000033EE000.00000004.00000800.00020000.00000000.sdmp, tchnhwrvi.exe, 00000002.00000002.567185811.0000000004F8C000.00000004.00000800.00020000.00000000.sdmp, tchnhwrvi.exe, 00000002.00000002.571773496.00000000075D0000.00000004.08000000.00040000.00000000.sdmp, tchnhwrvi.exe, 00000002.00000002.567185811.0000000004EA1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	tchnhwrvi.exe, 00000002.00000002.566066458.0000000003381000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.31.30.138	thesopranos.duckdns.org	United Kingdom		46261	QUICKPACKETUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	798336
Start date and time:	2023-02-03 23:16:11 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	15
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
Sample file name:	PhviZrlpkW.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/17@17/1
EGA Information:	• Successful, ratio: 100%

Copyright Joe Security LLC 2023

HDC Information:	• Successful, ratio: 14.9% (good quality ratio 14.3%) • Quality average: 82.8% • Quality standard deviation: 26%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.21
- Excluded domains from analysis (whitelisted): blobcollector.events.data.trafficmanager.net, onedsblobprdwus16.westus.cloudapp.azure.com, ctldl.windowsupdate.com, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
23:17:10	API Interceptor	934x Sleep call for process: tchnhwrvi.exe modified
23:17:10	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run rorscojuxn C:\Users\user\AppData\Roaming\ovawcpafrwk\edpm.exe "C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe" C:\Users\user\AppData\Loca
23:17:20	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run rorscojuxn C:\Users\user\AppData\Roaming\ovawcpafrwk\edpm.exe "C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe" C:\Users\user\AppData\Loca
23:17:34	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:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_edpm.exe_98859aec2feace66336d4eb3ad62fedc1a5d529e_aad16012_04aefae6\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9009185981848317
Encrypted:	false
SSDEEP:	96:samMF1rqNb2RhED7ZRNFpXIQcQ1Uc61dcElcw30vk+HbHg/5FAZugtYsaeOEXCkN:V7cbHQDfYvtjMGlq/u7syS274ltAT
MD5:	4C9B37DD98DEBA952CA651C113023767
SHA1:	7887DE1B1A6A583E01E1CDC5EBBE63BB4334C4FC
SHA-256:	DE3D30114334E4D0E04879F18702842677CC0C44096EBF3216286369E672B302
SHA-512:	B4453A4927711578D3A60ACF796EACFED4D453A7A0F0197E34C047143EB8F3981734D5E016244DC011E365B5C635E31EF87F1F87AE1DC2FCC70B63B1757BA7D2
Malicious:	false
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.=.1.3.3.1.9.9.3.6.2.4.4.3.3.7.1.5.3.2.....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.=.1.3.3.1.9.9.3.6.2.4.5.8.3.7.2.1.9.3.....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.=.2.b.1.2.0.6.8.1.-.b.b.9.9.-.4.3.d.c.-.8.9.4.a.-.9.5.d.0.e.5.0.e.e.b.5.0.....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.=.1.d.7.c.e.0.f.f.-.d.7.2.5.-.4.0.8.d.-.a.4.9.6.-.c.2.2.b.c.4.6.1.e.9.d.3.....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.=.e.d.p.m...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.9.a.4.-.0.0.0.1.-.0.0.1.f.-.6.0.8.9.-.a.1.4.7.1.d.3.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.a.3.e.9.2.b.c.b.c.a.a.a.3.b.2.b.0.b.c.8.6.1.a.c.d.9.5.9.8.9.8.0.0.0.0.f.f.f.f.!.0.0.0.0.5.6.e.0.2.2.2.b.9.d.0.2.5.c.c.d.b.4.f.f.d.6.b.e.4.4.3.e.c.1.1.d.0.4.2.d.4.9.9.3.!.e.d.p.m...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.3././.0.2././.0.1.:.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_edpm.exe_98859aec2feace66336d4eb3ad62fedc1a5d529e_aad16012_0e2afae6\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8944933806572445
Encrypted:	false
SSDEEP:	96:sFm9FFTuNb3RhED7ZRNFpXIQcQ1Uc61dcElcw30vk+HbHg5+5uHQ0DFF3V9w72/j:BnUCHQDfYvtjscPq/u7syS274ltAT
MD5:	C237F13C24934957828430FA85EE2978
SHA1:	FBC73199D8AAE59017DFD6F688B1C9407204B96E
SHA-256:	6E17F3B7FDA360093B4ED4B1E3E3B151B67619323F387C78A75874D8981FACEF
SHA-512:	195139294E3368FB93BBB011C2B12D0C0A3ED65E274CD825391D0926D604C93DB48AFDECCBE0B292D636E8DEDCBDA8799FEE3050739BDF05EC35FCCEA438B741
Malicious:	false
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.=.1.3.3.1.9.9.3.6.2.5.0.4.8.7.7.7.2.1.....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.=.1.3.3.1.9.9.3.6.2.5.1.4.2.5.3.1.8.2.....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.=.8.1.5.c.7.2.3.3.-.6.4.e.3.-.4.8.0.2.-.b.d.8.4.-.d.a.8.5.7.1.0.6.b.2.3.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.b.9.9.a.0.4.2.-.7.a.d.6.-.4.7.b.7.-.9.6.0.1.-.f.c.e.d.f.8.5.3.7.2.9.5.....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.=.e.d.p.m...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.1.3.f.0.-.0.0.0.1.-.0.0.1.f.-.4.7.d.c.-.8.5.4.d.1.d.3.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.a.3.e.9.2.b.c.b.c.a.a.a.3.b.2.b.0.b.c.8.6.1.a.c.d.9.5.9.8.9.8.0.0.0.0.f.f.f.f.!.0.0.0.0.5.6.e.0.2.2.2.b.9.d.0.2.5.c.c.d.b.4.f.f.d.6.b.e.4.4.3.e.c.1.1.d.0.4.2.d.4.9.9.3.!.e.d.p.m...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.3././.0.2././.0.1.:.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Feb 3 22:17:24 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	42040
Entropy (8bit):	2.024512213894416
Encrypted:	false
SSDEEP:	192:ofWJo53RwgHzOsQcNq8T+VZesgYgFSwBySXPV:5nsZ7GZesgYgFSw1f
MD5:	808457693416B37EAAACEECA1AEAEC7B
SHA1:	4A9D9E3EC429F09E83B23E7CB8A3AB679D2C1E4E
SHA-256:	D9533C0DBFA1E421D1151013B0A5F6A00AC33B64C59CE31BD7F8DB68858157BF
SHA-512:	499B65D56DBCF65367E0DDA6A43EBFA416897329D16A9E0785225C692746DB92E165429425CFBEE646D8B0421AE1F8E827945C04D12068AFC1F5711E298F1FDB
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....c.....P.....Z+.....T.....8.....T.....(.....U.....B.....p.....GenuineIntelW.....T.....c..... .....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\WERD405.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8322
Entropy (8bit):	3.686852809842928
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNilh6H6YeuSU2KEGgmf6S8+prZ89bo3sf4hYm:RrlsNij6H6YXSU2Agmf6Smo8f4L
MD5:	C47FB1BFB839DF2A251DAC5266C6E9A3
SHA1:	29342D732474A52AA8D7321189C1F8B276B3762C
SHA-256:	68BE108158A425B67822B9C7F5FBAAEA575948EA5F300BCD941BF96BA6D6829B
SHA-512:	AE6BCA833F2FE32E6E013E20E1FE87DAD09D0BA7CB015A9698A0C05267ECD42FD1C7BBB80166E4FD5B97739AE8DCFD00123253E84435A93EF769308DDDFBB4E8
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.4.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD445.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4622
Entropy (8bit):	4.403333093343135
Encrypted:	false
SSDEEP:	48:cvIwSD8zsVJgtWI9D/TWgc8sqYjja8fm8M4JH4FZ+q8vQ3IN1zCzd:uITfva/igrsqYvJUKG41zCzd
MD5:	7677B4D88DD3595FDD3354DAA341E362
SHA1:	03198DAFD342EBF9A54DD17EA90692679AF72353
SHA-256:	3A8B0111006362C92C0B6B7668CC8AC142E5AADE3D8FC021221BCBD7F6BF96E2
SHA-512:	2E31DD349090687C5EAC647D1B6BCCA28292FE426B47113CB73EF8370BDC805958A7B33DCCAF876356EE940EC3068C4B6617E2170EAE3281D3CED301DB70BA56
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1896928" />.. <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\WERE9EE.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Feb 3 22:17:30 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	40436
Entropy (8bit):	2.056282829146087
Encrypted:	false
SSDEEP:	192:ilfHniryTxFOoQc6pyqb02JzQXX6e7+V6pAocCA:sqoJNqb0KzsX6y+V6phA
MD5:	1FB3EEB01C764DABAE22F44D5E551ADE
SHA1:	2A2685BA4440D874B09998888DD32B41517DBEDF
SHA-256:	4342A5672DEF74E8D6A44A467C186DE7A2968AA94A37846E26641B95251E9597
SHA-512:	D4194BE3E79E69C0A5CE5C235AD5F1ED9670D565CD07BA119418C09D10B749E81313831DCEA65D5180A19EA6DEC14D3C9B233C22A0DB15E1A968B759C06F8AA
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....c.....*.....T.....8.....T.....I.....U.....B.....GenuineIntelW.....T.....c..... .....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\WEREC12.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8316
Entropy (8bit):	3.690400665517579
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNimMH6x6YelSUtlVzgmf6S8+pr789b0isfucm:RrlsNiF6x6YcSUtTgmf6Ss0hfM
MD5:	1B31096CBE7D3E726A599C9CC6C105DC
SHA1:	DC57E5F1AD6FDCCC9413466C3E2E567289A054AB
SHA-256:	2342825010A897DB92CA99D0E5152A2357D94781A5E600212A7C06B0E0D62726
SHA-512:	8238BBD8DBE58B01AB1581794741357E3F167C1C2AE2F8241FAE26AEE97EF8AFDBCA087C5707079AA01BDD3362D218BCDC3E465D8B573D9A923029FCC5134D F7
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.1.0. 4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC42.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4622
Entropy (8bit):	4.405035055172041
Encrypted:	false
SSDEEP:	48:cvIwSD8zsVJgtWI9D/TWgc8sqYj48fm8M4JH4FSz+q8vQ71zC2d:uITfva/igrsqYxJlKG1zC2d
MD5:	84250B7D1D034DB38E11A3F83DBE5A25
SHA1:	2C9AF8EB330B513D2C42C26980EE994E1F6D46E6
SHA-256:	E0E1A16228EA62FF2E12D7A2D9821C0F50948DC4EC0403DF952C09C4340275A4
SHA-512:	113313843B1AE96B5C6699CBE37A1A5085D0AFFAA359693F2B69B052C2213ECA5C431633A60AE512491F85F17E8EAA61D58F4F19120A7CF321495E0E51D29844
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1896928" />.. <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\Temp\lcrizgqjcc.mo	
Process:	C:\Users\user\Desktop\PhviZrlpkW.exe
File Type:	data
Category:	dropped
Size (bytes):	8155
Entropy (8bit):	7.182663154059607
Encrypted:	false
SSDEEP:	192:darcitQvArWiPvoob95WlOPrifKTndVi/sv6fLtNI7ypzV:uCYrNPvoavPrifKzdo06hNI7q
MD5:	67DF8B0B7F398320F69AA06DD324AABD
SHA1:	EFEA18F4A780A5BE154E40A5A9C8535782D11AF2
SHA-256:	244F2A16593E9A58DC56D66E8324BF0A019628C096CCF16D5355FF06265104CE
SHA-512:	61F103CDECAA9575E6FA5B6DD4922B0E992CF0B01D4004B554AD9127539513ED825B7BE02D12999D748F0E5F34D76666104B6D0A9822C03E5A1F43EA6767D01
Malicious:	false
Reputation:	low
Preview:	.705m..f.F<...05o.:.....?v>.3.3.<.....M.knl.02a..c.E<...42c. .....4.D63.6.3.?.....E.gni.53P..805.p8.q?.2.8.u .a..beabo.H0..v..v.@3.`..i/7.p.6.t(2..g.}.u<..G-.0.3.h.f....w8L$.m.r .D;F...okc..m.;4.q.?.<@.4.0...m..u<f...@%.`4..D'd.O$..A5..=..<r..4M.knl.82a..Q..401ec.t4.M4...D;.D..d580..E9....E....3.u.mje.18e..`W..480.x<.p=.4.4.p-P..6.c.!....D%.|.eX. ....+..t..0....e.a..`beP..580.p=.t>.8.5.p,XE..Md.....M9..e...@4.....F1..u.|c.....Lq.}<...v<+480.}<;.&<.>..r.^.q8F0....q.^.q8F0...^..M...3uc.....}<F...kloe.=8e....aboZf`Z\V.v...`ZY aZCV.v.j^YV.}.lZAU.w.`Z\^.q.iY.T.}.m^.q.[WIT.}....i.W.y.R.}.^.y.W.q.....XW..Mc.....\7!.K.y.a..`.....Z...Jo.....\GB.Gg.u.....X.B.Kg.v.....Pp..Nd.w.....\...Ke.}.....Y...Ko.p... ...G8.u....0<..480fP.401Y7a^?X580..D;.g.....A4...Tgn.`...G.X0P0.80..3cg.a.p0..D.`...igen.a..@.b.e.kX.013^3gR7]804p.F8.a.c..q.ad.G<n.`..D2..qb.e...knj..o.00`...)ecXg`Z]^.q .iYXk^OV.}.lZPU.w.`ZE^.q.iY]T.}.mR.R.t.IT.}._\hR.t...R.}.^.y.W.y.R.u.....ZR..Jo....\5$.O

C:\Users\user\AppData\Local\Temp\nse83F1.tmp

Process:	C:\Users\user\Desktop\PhviZrlpkW.exe
File Type:	data
Category:	dropped
Size (bytes):	412536
Entropy (8bit):	7.742692963191059
Encrypted:	false
SSDEEP:	12288:BRxkjTLz3xjDWVfJQ9qCU/vfVUgzshA4K9Wx:Ne9DGJQ9qXd4pKS
MD5:	45976AFF5588384336C2E3D34526DAC1
SHA1:	19586AA0CEA35DDEE5E7EFBE097A3E9BCE24C46D
SHA-256:	265CB23E00182EA146217F6E1F14AE29BA83C11D218F67CBEBE4668B165CE23D
SHA-512:	77A8205B700A90E46924FD1FE342D296A1BC9A2D5C8AE928090130CC6EE7F9B00078A8F9D79B753CE792E7F565967DC78222954845626D518F6FBCCBFFE2FD2
Malicious:	false
Preview:	.6.....,.....%.....5.....6.....T..... .....G.....K...j.....O.....p..... ....

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

Process:	C:\Users\user\Desktop\PhviZrlpkW.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82432
Entropy (8bit):	6.3796829712891165
Encrypted:	false
SSDEEP:	1536:VAYSS9siqxKZXtrcbYoo526WlHgnlcdrzDSQnABsScD9:+YdyxKzxWxsScD
MD5:	64F982758878F6A97ED4B3D99CFBD371
SHA1:	56E0222B9D025CCDB4FFD6BE443EC11D042D4993
SHA-256:	BE58EBBA3239A9AF70FD8E1FFDF426EA89855574FF8B38794262D445B4EB351B
SHA-512:	BA592967E39EE53682CDF87A9BDD943F536321D1014DF1139531B73AF28B71CE596175B698A090E4306F7BB0C86694B822A1B57E13A879DD034F3ADED6E5D11
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 65% • Antivirus: Virustotal, Detection: 52%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%..}K.}K.}K.....}K.....}K.....}K....}K.}J..}K.....}K.....}K.Rich.}K..... .....PE..L...+U.c.....q5.....@.....@.....#.....|..... ....text..... ..`.rdata...1.....2.....@..@.data....B...@.....@....reloc.....@..B..... ....

C:\Users\user\AppData\Local\Temp\tthfqfao.aa

Process:	C:\Users\user\Desktop\PhviZrlpkW.exe
File Type:	data
Category:	dropped
Size (bytes):	307935
Entropy (8bit):	7.985923940553015
Encrypted:	false
SSDEEP:	6144:2hXx4RjTF5mqJlX4e3DljJJ3WJPksJQrCQXq1IzQ1/V/HnPfYuUJSrk:2RxkjTLz3xjDWVfJQ9qCU/vfVUp
MD5:	ED01FB080A7C07E4B8ADEC8148D0C434
SHA1:	81474DD1BD248E9D080D55495DB795B4C52CC57D
SHA-256:	AAAFF8393BFBBB2AD8865ECBEC0989162825F52184FB305FB0846D0C2C0D9654
SHA-512:	F5FB047014EB631A0EA91064D0C440A9489F50CC4160DBAC507AEBD5B58D752112F1C69AE15F81A136C51D962FE4E478CDEC52C8A9B7411C110076C09F99EA8
Malicious:	false
Preview:	.....+V..e. .@...N;.:R....9(..6&._...kj.A...eL.a.d.....-.....zx#..p.....j..j...>!.%8...)~..'Q.T.A...-....P..c...../b...e@.KKX.=....k....r...T_.....".L.g!....q....N3...+.td.,.f >.bs..R,..]4W.. .G@G...k`.LF...q.7Ih.....>]8..4..x.]...{.....+M..e!.C@....N;.:.....9."[t._...kcAA...ez.a.dM.....>.....j..n.{...0..O.D..(..2[@.t.o ..A..e.R...?...ZM&.c .....M.g.N^.t.5...p..&.+.u.;. .....mLW.2..<..9...a.....).iHE&E.c..Y{"b..\3..5..F"3...#...y.()u.{.....'Y...pA..[.3.x.]...{...Yq..+...e...@....NC.:.....9(..6&.....J.3..ewFa.d.....m..>5...].....n...].q%.O.4/.(..b[@nt...OiA.. e.?.....fZ..I7....l....1OM..5N\./.5w3....&.+.u.;.....mLW.2..<..j...2.a.....).iHE&E.c..Y{"b..\3..M..."3...#...y.(pu.....'Y...pA..[.3.x.]...{.....+...e.p.@....N;.:.....9(..6&._...kj.A...eL.a.d. .....>5...].....n.{...0..O.Dv.(..2[@.t.. .iA..e.?.....fZM&.c.....M..oN\.t.5w3....&.+.u.;. .....mLW.2..<..j...2.a.....).iHE&E.c..Y{"b..\3..M..."3...#...y.(pu.....

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat

Process:	C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe

File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35(A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:OjS:Ou
MD5:	FDECF7936CC694269FF8F1961A68ADBB
SHA1:	0BC2E2B015FB7A83E00CD0C8CFE08D25B5A60F6D
SHA-256:	D1629F7944B42A620D3D35FFAA86125EC31C4E57D57EC0408CD71BCCD86E1E5B
SHA-512:	A010C551B8E6885B903A388CC90579A8D5FAD24C900CA813DD044C57CED4B36E8812FD5FE9B57C0420DBBF8574BDEF2D6342FAC1C89C2207D2FC9E8127BF9EF
Malicious:	**true**
Preview:	...d4..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin

Process:	C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44F8
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat

Process:	C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPlZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E926

Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v."".v.......#..X.a...../...cC...i..l{>5n._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.I.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\ovawcpafrwk\edpm.exe

Process:	C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	82432
Entropy (8bit):	6.3796829712891165
Encrypted:	false
SSDEEP:	1536:VAYSS9siqxKZXtrcbYoo526WIHgnlcdrzDSQnABsScD9:+YdyxKzxWxsScD
MD5:	64F982758878F6A97ED4B3D99CFBD371
SHA1:	56E0222B9D025CCDB4FFD6BE443EC11D042D4993
SHA-256:	BE58EBBA3239A9AF70FD8E1FFDF426EA89855574FF8B38794262D445B4EB351B
SHA-512:	BA592967E39EE53682CDF87A9BDD943F536321D1014DF1139531B73AF28B71CE596175B698A090E4306F7BB0C86694B822A1B57E13A879DD034F3ADED6E5D11
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 65% • Antivirus: Virustotal, Detection: 52%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%..}K.}K.}K.....}K.....}K.....}K....}K.}J..}K.....}K.....}K.Rich.}K..... .....PE..L...+U.c.....q5.....@.....@.....#.....|..... ....text..... ..`.rdata...1.....2.....@..@.data....B...@.....@....reloc.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.1512123375745995
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:	PhviZrlpkW.exe
File size:	775369
MD5:	565044691fedb39980cb814dc26f9ebd
SHA1:	d92f48359c385fd03a419e583495ead52428654e
SHA256:	3a1c1eabfbe52d5a822e95462e730775ea9eef9d8d653f3a1ff6904378ad3e0c
SHA512:	ee459c0234c40c4b353f9ea6dbdb8297adac7b63727fb5bcfefbfa2404e0d14882d48656caf8f62897cba00cf7de20da19eb638bc3530e8d13fdb85cfaf58b3c
SSDEEP:	6144:8Ya6SW0O0WqiBiGei7FTjUosytWnSS1SqY7WnoVhcOdN3eJznS/FK0Y4Zh/9VR9A:8Y6WqyTT5WnoLX9dK0XZh1RYCChaWKDW
TLSH:	73F4E0537A00B2E5D8B044397C1AC1F34B99AE3999543E573AD4BF3F38B5123960A73A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	fcd4dcc4f0797979

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x614F9B1F [Sat Sep 25 21:56:47 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F3638DF5C5Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F3638DF5C2Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax

Instruction
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0x64f00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.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	0x6676	0x6800	False	0.6568134014423077	data	6.4174599871908855	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.141066817170598	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.110582127654237	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3b000	0x64f00	0x65000	False	0.2831088528774752	data	3.743561491677653	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b328	0x42028	Device independent bitmap graphic, 256 x 512 x 32, image size 262144	English	United States
RT_ICON	0x7d350	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States
RT_ICON	0x8db78	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864	English	United States
RT_ICON	0x97020	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0x9b248	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x9d7f0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0x9e898	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	English	United States
RT_ICON	0x9f220	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_DIALOG	0x9f688	0x100	data	English	United States
RT_DIALOG	0x9f788	0x11c	data	English	United States
RT_DIALOG	0x9f8a8	0x60	data	English	United States
RT_GROUP_ICON	0x9f908	0x76	data	English	United States
RT_VERSION	0x9f980	0x23c	data	English	United States
RT_MANIFEST	0x9fbc0	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

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

Network Behavior

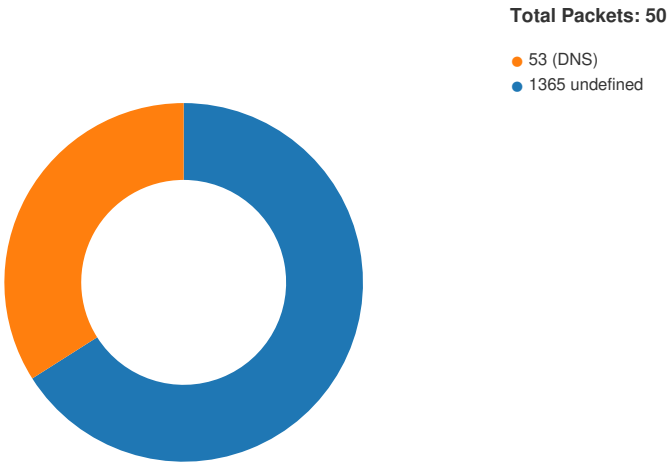
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4193.31.30.138 4972613652816766 02/03/23-23:19:06.285273	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49726	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4971313652816766 02/03/23-23:17:46.673206	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49713	1365	192.168.2.4	193.31.30.138

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4193.31.30.138 4971813652816766 02/03/23-23:18:21.376630	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49718	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4972113652816766 02/03/23-23:18:33.469715	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49721	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4971613652816766 02/03/23-23:18:07.532553	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49716	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4971413652816766 02/03/23-23:17:53.669627	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49714	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4972313652816766 02/03/23-23:18:47.034655	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49723	1365	192.168.2.4	193.31.30.138
193.31.30.138192.168.2.4 1365497022810290 02/03/23-23:17:30.731633	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	1365	49702	193.31.30.138	192.168.2.4
192.168.2.4193.31.30.138 4972513652816718 02/03/23-23:18:58.945928	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49725	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4970213652816766 02/03/23-23:17:32.574212	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49702	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4971713652816766 02/03/23-23:18:13.577404	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49717	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4971413652816718 02/03/23-23:17:52.672539	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49714	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4971213652816766 02/03/23-23:17:40.364031	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49712	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4972213652816766 02/03/23-23:18:41.032521	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49722	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4972513652816766 02/03/23-23:18:59.896530	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49725	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4969313652816766 02/03/23-23:17:25.471865	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49693	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4971513652816766 02/03/23-23:18:01.525116	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49715	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4969113652816766 02/03/23-23:17:14.041382	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49691	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4972013652816766 02/03/23-23:18:27.458779	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49720	1365	192.168.2.4	193.31.30.138
192.168.2.4193.31.30.138 4972413652816766 02/03/23-23:18:53.018271	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49724	1365	192.168.2.4	193.31.30.138

Network Port Distribution

Copyright Joe Security LLC 2023



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2023 23:17:12.300127029 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.330926895 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.331037998 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.413235903 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.450130939 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.459686995 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.490725040 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.533387899 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.602159023 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.602196932 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.602216959 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.602238894 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.602257967 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.602314949 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.602349997 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.633047104 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.633085012 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.633105040 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.633125067 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.633155107 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.633167982 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.633177996 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.633197069 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.633215904 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.633235931 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.633251905 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.633261919 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.633284092 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.664132118 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664169073 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664189100 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664208889 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664230108 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664251089 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664272070 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664295912 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664321899 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.664343119 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.664355993 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664361954 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.664381027 CET	1365	49691	193.31.30.138	192.168.2.4

Copyright Joe Security LLC 2023

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2023 23:17:12.664398909 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664417982 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664436102 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.664446115 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664464951 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.664474010 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664491892 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664510965 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664525986 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.664537907 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.664560080 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.695408106 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695442915 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695462942 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695485115 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695504904 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695522070 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.695548058 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695557117 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.695575953 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695589066 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.695605040 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695625067 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695646048 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695671082 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695678949 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.695699930 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695708990 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.695729017 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695739985 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.695759058 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695779085 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695799112 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695817947 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.695828915 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695847034 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.695858955 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695879936 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695900917 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695918083 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.695930958 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695944071 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.695959091 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.695980072 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.696002007 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.696022987 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.696033001 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.696053028 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.696062088 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.696079969 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.696095943 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.696108103 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.696127892 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.696147919 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.696166039 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.696176052 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.696194887 CET	1365	49691	193.31.30.138	192.168.2.4
Feb 3, 2023 23:17:12.696202993 CET	49691	1365	192.168.2.4	193.31.30.138
Feb 3, 2023 23:17:12.726975918 CET	1365	49691	193.31.30.138	192.168.2.4

Copyright Joe Security LLC 2023

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2023 23:17:12.182507992 CET	57417	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:17:12.291882038 CET	53	57417	8.8.8.8	192.168.2.4
Feb 3, 2023 23:17:23.454297066 CET	50982	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:17:23.471971989 CET	53	50982	8.8.8.8	192.168.2.4
Feb 3, 2023 23:17:30.550218105 CET	64167	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:17:30.658106089 CET	53	64167	8.8.8.8	192.168.2.4
Feb 3, 2023 23:17:37.685573101 CET	56807	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:17:37.703191042 CET	53	56807	8.8.8.8	192.168.2.4
Feb 3, 2023 23:17:45.607497931 CET	61007	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:17:45.716548920 CET	53	61007	8.8.8.8	192.168.2.4
Feb 3, 2023 23:17:51.722161055 CET	60686	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:17:51.830809116 CET	53	60686	8.8.8.8	192.168.2.4
Feb 3, 2023 23:17:59.174943924 CET	61124	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:17:59.283678055 CET	53	61124	8.8.8.8	192.168.2.4
Feb 3, 2023 23:18:06.551378012 CET	59444	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:18:06.569550037 CET	53	59444	8.8.8.8	192.168.2.4
Feb 3, 2023 23:18:12.558892965 CET	55570	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:18:12.576698065 CET	53	55570	8.8.8.8	192.168.2.4
Feb 3, 2023 23:18:18.683300018 CET	64906	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:18:18.792500019 CET	53	64906	8.8.8.8	192.168.2.4
Feb 3, 2023 23:18:26.458391905 CET	50861	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:18:26.478123903 CET	53	50861	8.8.8.8	192.168.2.4
Feb 3, 2023 23:18:32.484534025 CET	61088	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:18:32.502001047 CET	53	61088	8.8.8.8	192.168.2.4
Feb 3, 2023 23:18:39.776468992 CET	58729	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:18:39.884972095 CET	53	58729	8.8.8.8	192.168.2.4
Feb 3, 2023 23:18:46.066214085 CET	64700	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:18:46.175755024 CET	53	64700	8.8.8.8	192.168.2.4
Feb 3, 2023 23:18:52.083476067 CET	56022	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:18:52.192724943 CET	53	56022	8.8.8.8	192.168.2.4
Feb 3, 2023 23:18:58.731571913 CET	60822	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:18:58.748497009 CET	53	60822	8.8.8.8	192.168.2.4
Feb 3, 2023 23:19:04.980493069 CET	49750	53	192.168.2.4	8.8.8.8
Feb 3, 2023 23:19:05.089649916 CET	53	49750	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 3, 2023 23:17:12.182507992 CET	192.168.2.4	8.8.8.8	0x82cc	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:17:23.454297066 CET	192.168.2.4	8.8.8.8	0xe8d3	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:17:30.550218105 CET	192.168.2.4	8.8.8.8	0x3e21	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:17:37.685573101 CET	192.168.2.4	8.8.8.8	0x16d7	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:17:45.607497931 CET	192.168.2.4	8.8.8.8	0x2ba3	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:17:51.722161055 CET	192.168.2.4	8.8.8.8	0xec96	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:17:59.174943924 CET	192.168.2.4	8.8.8.8	0xc842	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:06.551378012 CET	192.168.2.4	8.8.8.8	0x8297	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:12.558892965 CET	192.168.2.4	8.8.8.8	0xcf26	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:18.683300018 CET	192.168.2.4	8.8.8.8	0x61ec	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:26.458391905 CET	192.168.2.4	8.8.8.8	0x78b2	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false

Copyright Joe Security LLC 2023

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 3, 2023 23:18:32.484534025 CET	192.168.2.4	8.8.8.8	0xb12b	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:39.776468992 CET	192.168.2.4	8.8.8.8	0x4a72	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:46.066214085 CET	192.168.2.4	8.8.8.8	0xc722	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:52.083476067 CET	192.168.2.4	8.8.8.8	0xfba4	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:58.731571913 CET	192.168.2.4	8.8.8.8	0x5fcb	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:19:04.980493069 CET	192.168.2.4	8.8.8.8	0xc980	Standard query (0)	thesoprano s.duckdns.org	A (IP address)	IN (0x0001)	false

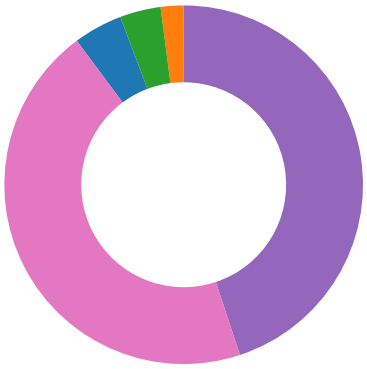
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 3, 2023 23:17:12.291882038 CET	8.8.8.8	192.168.2.4	0x82cc	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:17:23.471971989 CET	8.8.8.8	192.168.2.4	0xe8d3	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:17:30.658106089 CET	8.8.8.8	192.168.2.4	0x3e21	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:17:37.703191042 CET	8.8.8.8	192.168.2.4	0x16d7	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:17:45.716548920 CET	8.8.8.8	192.168.2.4	0x2ba3	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:17:51.830809116 CET	8.8.8.8	192.168.2.4	0xec96	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:17:59.283678055 CET	8.8.8.8	192.168.2.4	0xc842	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:06.569550037 CET	8.8.8.8	192.168.2.4	0x8297	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:12.576698065 CET	8.8.8.8	192.168.2.4	0xcf26	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:18.792500019 CET	8.8.8.8	192.168.2.4	0x61ec	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:26.478123903 CET	8.8.8.8	192.168.2.4	0x78b2	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:32.502001047 CET	8.8.8.8	192.168.2.4	0xb12b	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:39.884972095 CET	8.8.8.8	192.168.2.4	0x4a72	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:46.175755024 CET	8.8.8.8	192.168.2.4	0xc722	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:52.192724943 CET	8.8.8.8	192.168.2.4	0xfba4	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:18:58.748497009 CET	8.8.8.8	192.168.2.4	0x5fcb	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false
Feb 3, 2023 23:19:05.089649916 CET	8.8.8.8	192.168.2.4	0xc980	No error (0)	thesoprano s.duckdns.org		193.31.30.138	A (IP address)	IN (0x0001)	false

Copyright Joe Security LLC 2023

Statistics

Behavior



PhviZrlpkW.exe
tchnhwrvi.exe
tchnhwrvi.exe
edpm.exe
WerFault.exe
edpm.exe
WerFault.exe

Click to jump to process

System Behavior

Analysis Process: PhviZrlpkW.exe PID: **4624**, Parent PID: **3528**

General

Target ID:	0
Start time:	23:17:04
Start date:	03/02/2023
Path:	C:\Users\user\Desktop\PhviZrlpkW.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PhviZrlpkW.exe
Imagebase:	0x400000
File size:	775369 bytes
MD5 hash:	565044691FEDB39980CB814DC26F9EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsu83B2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nse83F1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nse83F2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW

Copyright Joe Security LLC 2023

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
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	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nse83F2.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405BE2	CreateDirectoryW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
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	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\tthfqfao.aa	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\lcrizgqjcc.mo	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsu83B2.tmp	success or wait	1	403988	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nse83F2.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nse83F1.tmp	0	28580	fd 36 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 02 00 00 00 fd 11 00 00 fd 00 00 00 1c 25 00 00 00 00 00 00 fd 35 00 00 01 00 00 00 fd 36 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 54 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	6,%56T	success or wait	21	406224	WriteFile
C:\Users\user\AppData\Local\Temp\tthfqfao.aa	0	16384	05 fd 1d fd 0c 2b 56 fd fd 65 10 20 18 40 fd fd fd 4e 3b 18 3a 52 00 06 09 fd 39 28 fd fd 36 26 fd 5f fd fd fd 6b 6a fd 41 09 fd fd 65 4c fd 61 fd 64 fd fd fd fd fd 09 fd fd 2d fd 7d fd fd 80 fd fd fd fd 7a 78 23 7f fd 70 fd fd d5 fd fd 6a fd 01 6a fd 11 fd 3e 21 fd 25 38 fd fd fd 29 7e 1a fd 27 51 c9 54 fd 41 0c fd fd 2d fd 0f fd fd 50 fd fd 63 fd fd 02 fd 25 fd 2f 62 ac fd fd 65 40 fd 4b 4b 58 fd 3d fd fd fd fd 6b fd ab fd 0c 72 05 3f 07 54 5f fd fd fd fd fd fd 22 fd 4c fd 67 21 fd fd 14 0d 71 fd fd fd fd 4e 33 fd fd 0c 2b fd 74 64 12 2c 00 66 20 3e fd 62 73 fd fd 52 2c fd fd 5d 34 57 7f 13 fd 47 40 47 0d 08 fd 6b 60 00 4c 46 fd 0d fd 71 fd 37 49 68 fd fd fd fd fd 3e 5d 38 fd fd 34 fd fd 78 15 5d 13 fd fd	+Ve @N;:R9(6&_kjAeLad-zx#pjj>!%8)~'QTA-Pc/be@KKX=krT_"Lg!qN 3+td,f >bsR,]4WG@Gk`LFq7Ih >]84x]	success or wait	19	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lcrizgqjcc.mo	0	8155	e3 37 30 35 6d fd fd 66 fd 46 3c fd 12 1b 30 35 6f fd 3a fd fd fd fd fd 3f 76 3e fd 33 fd 33 fd 3c fd 0c fd fd fd fd 4d fd 6b 6e 6c fd 30 32 61 fd fd 63 fd 45 3c fd 17 10 34 32 63 fd 20 fd fd fd fd fd 34 fd 44 36 33 fd 36 fd 33 fd 3f fd 0d fd fd fd 45 fd 67 6e 69 fd 35 33 50 fd 04 38 30 35 fd 70 38 fd 71 3f fd 32 fd 38 fd 75 20 fd 61 fd fd 62 65 61 62 6f fd 48 30 03 bb 76 0f fd 76 0c 40 33 fd 60 14 fd 69 2f 37 fd 70 14 36 fd 74 28 32 fd fd 67 31 7d 71 75 3c fd fd 47 2d fd 30 fd 33 fd 68 fd 66 fd fd fd 0f 77 38 4c 24 fd 6d fd 72 0b 44 3b 46 fd 07 fd 6f 6b 63 fd fd 6d fd 3b 34 fd 71 fd 3f fd 3c 40 fd 34 fd 30 fd fd fd 6d fd 73 75 3c 66 fd f1 fd 40 25 fd 60 34 fd fd 44 27 64 fd 4f 24 fd fd 41 35 1b fd 3d 01 fd 3c 72 fd	705mfF<05o:? v>33<Mknl02acE<42c 4D6363? Egni53P805p8q?28u abea boH0vv@3`i/7p6t(2g}u<G -03hfw8L $mrD;Fokcm;4q? <@40mu<f@%`4D'dO $A5=<r	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 1c 25 fd fd 7d 4b d8 7d 4b d8 7d 4b fd fd 0b fd f8 7d 4b fd fd 0b fd cb 7d 4b fd fd 0b fd fd fd 7d 4b d1 05 fd cf 7d 4b d8 7d 4a fd 07 7d 4b fd fd 0b fd d9 7d 4b fd fd 0b fd d9 7d 4b fd 52 69 63 68 fd 7d 4b fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 2b 55 fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0a 00 00 fd 00	MZ@!L!This program cannot be run in DOS mode.$%}K}K}K}K}K}K}J}K}K}KRich}KPEL+Uc	success or wait	6	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PhviZrlpkW.exe	unknown	512	success or wait	876	4061F5	ReadFile
C:\Users\user\Desktop\PhviZrlpkW.exe	unknown	16384	success or wait	20	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nse83F1.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nse83F1.tmp	unknown	13998	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nse83F1.tmp	unknown	4	success or wait	3	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nse83F1.tmp	unknown	16384	success or wait	26	4061F5	ReadFile

Analysis Process: tchnhwrvi.exe PID: **2120**, Parent PID: **4624**

General

Target ID:	1
Start time:	23:17:04
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe
Wow64 process (32bit):	true

Copyright Joe Security LLC 2023

Commandline:	"C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe" C:\Users\user\AppData\Local\Temp\lcrizgqjcc.mo
Imagebase:	0x280000
File size:	82432 bytes
MD5 hash:	64F982758878F6A97ED4B3D99CFBD371
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.309024218.0000000000B00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.309024218.0000000000B00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.309024218.0000000000B00000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.309024218.0000000000B00000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.309024218.0000000000B00000.00000004.00001000.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.309024218.0000000000B00000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 65%, ReversingLabs • Detection: 52%, Virustotal, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ovawcpafrwk	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5F0414	CreateDirectoryW
C:\Users\user\AppData\Roaming\ovawcpafrwk\edpm.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5F0357	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ovawcpafrwk\edpm.exe	0	82432	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 fd 1c 25 fd fd 7d 4b d8 7d 4b d8 7d 4b fd fd 0b fd f8 7d 4b fd fd 0b fd cb 7d 4b fd fd 0b fd fd fd 7d 4b d1 05 fd cf 7d 4b d8 7d 4a fd 07 7d 4b fd fd 0b fd d9 7d 4b fd fd 0b fd d9 7d 4b fd 52 69 63 68 fd 7d 4b fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 2b 55 fd 63 00 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0a 00 00 fd 00	MZ@!L!This program cannot be run in DOS mode.$%}K}K}K}K}K}K}K}J}K}K}KRich}KPEL+Uc	success or wait	1	5F0366	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lcrizgqjcc.mo	unknown	4096	success or wait	1	285205	ReadFile
C:\Users\user\AppData\Local\Temp\lcrizgqjcc.mo	unknown	4096	success or wait	1	285205	ReadFile
C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe	unknown	82432	success or wait	1	5F0339	ReadFile
C:\Users\user\AppData\Local\Temp\tthfqfao.aa	unknown	287232	success or wait	1	5F121D	ReadFile

Copyright Joe Security LLC 2023

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	5F17FC	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	5F17FC	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	5F17FC	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	5F17FC	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	5F17FC	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	5F17FC	ReadFile

Registry Activities

Analysis Process: tchnhwrvi.exe

PID: **1312**, Parent PID: **2120**

General

Target ID:	2
Start time:	23:17:06
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe
Imagebase:	0x280000
File size:	82432 bytes
MD5 hash:	64F982758878F6A97ED4B3D99CFBD371
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.567185811.0000000004E2C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.567185811.0000000004E2C000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.567185811.0000000004E2C000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.564994074.0000000001587000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.564994074.0000000001587000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.564994074.0000000001587000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.564994074.0000000001587000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.571891406.0000000007620000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.571891406.0000000007620000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.571891406.0000000007620000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.571891406.0000000007620000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.571954055.0000000007660000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.571954055.0000000007660000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.571954055.0000000007660000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.571954055.0000000007660000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000003.317149940.0000000006A39000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.571812469.00000000075F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.571812469.00000000075F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.571812469.00000000075F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.571812469.00000000075F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.564427693.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.564427693.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.564427693.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.564427693.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.564427693.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.564427693.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.570983718.0000000005DF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.570983718.0000000005DF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.570983718.0000000005DF0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.570983718.0000000005DF0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.570983718.0000000005DF0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.571761394.00000000075C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.571761394.00000000075C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.571761394.00000000075C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.571761394.00000000075C0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.571720723.0000000007590000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.571720723.0000000007590000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.571720723.0000000007590000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.571720723.0000000007590000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.567185811.00000000043A5000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.571671329.0000000007570000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.571671329.0000000007570000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.571671329.0000000007570000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.571671329.0000000007570000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.567185811.0000000004404000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.567185811.0000000004404000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.571793197.00000000075E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.571793197.00000000075E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.571793197.00000000075E0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.571793197.00000000075E0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.567185811.0000000004C83000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.567185811.0000000004C83000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.567185811.0000000004C83000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.571026013.0000000005E10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.571026013.0000000005E10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.571026013.0000000005E10000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.571026013.0000000005E10000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.571773496.00000000075D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.571773496.00000000075D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.571773496.00000000075D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.571773496.00000000075D0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.566066458.00000000033EE000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.566066458.00000000033EE000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.571597397.00000000073F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.571597397.00000000073F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.571597397.00000000073F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.571597397.00000000073F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.565935661.0000000003332000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.565935661.0000000003332000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.565935661.0000000003332000.00000040.00001000.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.565935661.0000000003332000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.571745163.00000000075B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.571745163.00000000075B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.571745163.00000000075B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.571745163.00000000075B0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.566066458.0000000003381000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.571864347.0000000007610000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.571864347.0000000007610000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.571864347.0000000007610000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.571864347.0000000007610000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.570873526.0000000005BB0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.570873526.0000000005BB0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.570873526.0000000005BB0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.570873526.0000000005BB0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.567185811.0000000004F8C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.567185811.0000000004F8C000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.567185811.0000000004F8C000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.567185811.0000000004EA1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.567185811.0000000004EA1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.565592440.0000000003290000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.565592440.0000000003290000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.565592440.0000000003290000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.565592440.0000000003290000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.565592440.0000000003290000.00000004.08000000.00040000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.565592440.0000000003290000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

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	72E1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C6BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	16	71C61E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd fd fd 64 34 06 fd 48	d4H	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	17	71C61B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327432	70 54 eb fd 21 fd 08 57 fd fd 47 14 4a fd fd 61 60 29 17 40 8b 69 fd fd 77 70 4b fd 73 6f 40 fd 06 fd 35 fd 3d 10 5e fd 1d 51 fd 6f 79 fd 3d 65 40 39 fd 42 fd fd fd 46 fd fd 30 39 75 22 33 fd fd 20 30 74 fd 19 52 44 6e 5f 34 64 fd fd 17 02 fd 45 fd fd 06 69 fd 08 fd fd fd fd 7e 0c fd fd 7c fd fd 66 58 5f 0e fd fd 58 66 fd 70 5e fd fd fd fd 03 fd 3e 61 cb fd 24 fd fd fd 65 05 36 3a 37 64 fd 28 61 05 41 fd fd fd 3d fd 29 2a 0d fd fd fd fd 7b 42 1c 5b fd fd fd 79 25 fd 2a 31 fd 69 fd 51 fd 3c 12 90 78 74 29 58 13 11 48 09 fd 20 fd 24 48 46 37 67 0f fd fd 49 fd 2a 33 03 7b 0c 6e fd fd fd fd 4c 5b 79 3b 69 fd fd 73 2d 1e fd fd fd 28 35 69 8b fd fd 10 fd fd 02 fd fd 08 17 4a 09 35 62 37 7d fd fd 66 4b fd fd 48 56	pT!WGJa)@iwpKso@5=^ Qoy=e@9BF09u"3 0tRDn_4dEi~|fX_Xfp^>a$ e6:7d(aA=)* {B[y%*iQ<xtXH HF7gI*3{nLy;is- (5iJ5b7}fKHV	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d fd 16 fd fd 20 38 fd 6a fd fd fd fd 7c fd 26 58 fd fd 65 fd 46 fd 2a fd	9iH}Z4f 8j|&XeF*	success or wait	1	71C61B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: edpm.exe PID: **2468**, Parent PID: **3528**

General

Target ID:	3
Start time:	23:17:19
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Roaming\ovawcpafrwk\edpm.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\ovawcpafrwk\edpm.exe" "C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe" C:\Users\user\AppData\Loca
Imagebase:	0x1d0000
File size:	82432 bytes
MD5 hash:	64F982758878F6A97ED4B3D99CFBD371
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 65%, ReversingLabs • Detection: 52%, Virustotal, Browse
Reputation:	low

Analysis Process: WerFault.exe PID: **1256**, Parent PID: **2468**

General

Target ID:	6
Start time:	23:17:23
Start date:	03/02/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2468 -s 656
Imagebase:	0x980000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D2A1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD445.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD445.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_edpm.exe_98859aec2feace66336d4eb3ad62fedc1a5d529e_aad16012_04aefae6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_edpm.exe_98859aec2feace66336d4eb3ad62fedc1a5d529e_aad16012_04aefae6\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D29497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD445.tmp	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD445.tmp.xml	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD462.tmp.csv	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD713.tmp.txt	success or wait	1	6D29497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.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 63 fd 05 12 00 00 00 00 00	MDMP c	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	7024	6	00 00 00 00 00 00		success or wait	1	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.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 70 1b 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 09 00 00 fd fd 63 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 20 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	UBpGenuineIntelWTc W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	8234	716	01 00 01 00 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 22 00 00 00 fd 2b 00 00 01 53 00 4c 01 2b 00 00 00 2b 00 4c 01 fd 66 71 74 17 04 00 fd 02 00 00 00 00 00 00 00 00 00 00 00 fd fd 2f 01 fd fd 2f 01 66 3c 1d 00 23 00 fd 77 16 02 00 00 5c 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	!"+SL++Lfqt//f<#w\/+	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	1620	168	fd 17 00 00 00 00 00 00 17 04 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 66 3c 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 2a 20 00 00	f<*	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	11098	20	0e 00 00 00 fd 3b 1d 00 00 00 00 00 00 01 00 00 3e 2c 00 00	;>,	success or wait	14	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	11326	256	30 fd fd fd 01 00 01 00 fd fd fd fd fd fd fd 49 fd fd fd fd fd fd fd 4d 0c fd fd fd fd fd fd 4d 10 fd fd fd fd fd fd fd fd fd fd fd fd 15 18 01 1e 00 6a 00 fd fd fd 15 1c 01 1e 00 fd fd fd fd fd fd 50 fd 15 20 01 1e 00 fd fd 75 10 fd fd 75 0c fd fd fd 74 07 53 fd 77 3d 00 00 59 fd 4d fd 5f 33 fd 5b fd 72 3d 00 00 fd cb fd 56 6a 01 fd 17 04 00 fd 56 6a 02 fd fd fd fd fd fd fd 0c 56 fd 15 08 01 1e 00 50 fd 15 0c 01 1e 00 5e cb fd 55 fd fd fd 35 fd 51 1e 00 fd 15 10 01 1e 00 fd fd 74 03 5d fd fd fd 75 18 fd 75 14 fd 75 10 fd 75 0c fd 75 08 fd fd fd fd fd 33 fd 50 50 50 50 50 fd fd fd fd fd fd fd 14 cb fd 55 fd fd 45 08 33 fd 3b 04 50 42 1e 00 74 13 41 fd fd 2d 72 fd 48 fd fd 11 77 0e 6a 0d 58 5d cb 04 54 42 1e 00 5d fd	0IMMjP uutSw=YM_3[r=VjVjVP^ U5Q t]uuuuu3PPPPPUE3;BtA-rHwjX]B]	success or wait	13	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	30566	2120	fd fd fd 77 fd fd fd 77 fd 00 00 00 fd fd fd fd 10 00 00 00 4c fd 6b 01 18 fd 6b 01 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd 00 fd 04 01 00 fd 04 01 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd 04 01 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 6f 4c 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 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd 10 56 4d 01 00 00 00 00 00 00 00 00 68 6b 4c 01 00 fd 04 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 00 00 00 fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd 50 fd 7b 01 54 fd 04 01 58 fd 7b 01 fd 6f 4c 01 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwLkk@w@woLVMhkLP {TX{oL	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	8950	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 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 2f 01 fd fd fd 77 23 00 00 00 16 02 00 00 00 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	?+S++/w#/+	success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	1888	48	fd 17 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 05 01 00 00 00 00 fd fd 7b 01 00 00 00 00 7c 09 00 00 fd 61 00 00 fd 02 00 00 fd 28 00 00	{|a(	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	1948	4	29 00 00 00	)	success or wait	41	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	7030	22	10 00 00 00 65 00 64 00 70 00 6d 00 2e 00 65 00 78 00 65 00 00 00	edpm.exe	success or wait	41	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	6272	752	00 00 fd 76 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 12 20 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 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 01 03 00 00 00 00 62 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 0e 7f 03 00 00 00 00 00 2f fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 11 1b 00 00 00 00 00 59 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 32 06 00 00 00 00	v`A!-a BB?#@AZbb/Y@2	success or wait	1	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	32686	9354	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 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1E2.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 50 11 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 5a 2b 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 28 1a 00 00 10 fd 00 00 15 00 00 00 fd 01 00 00 fd 18 00 00 16 00 00 00 fd 00 00 00 fd 1a 00 00	PZ+T8T(	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D29497A	unknown

Copyright Joe Security LLC 2023

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 32 00 34 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>2468</Pid>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 64 00 70 00 6d 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>edpm.exe</ImageName>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1072	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 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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1170	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 37 00 37 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5772</Uptime>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1212	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1216	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1220	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1302	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1306	2	09 00		success or wait	2	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1310	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1362	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1366	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1370	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1414	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1418	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1424	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 38 00 39 00 37 00 34 00 37 00 34 00 35 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>89747456</PeakVirtualSize>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1510	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1514	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1520	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 38 00 38 00 34 00 34 00 30 00 38 00 33 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>88440832</VirtualSize>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1590	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1594	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1600	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 38 00 38 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>1888</PageFaultCount>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1674	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1678	2	09 00		success or wait	3	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1684	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 32 00 34 00 35 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7245824</PeakWorkingSetSize>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1780	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1784	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1790	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 32 00 34 00 35 00 38 00 32 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>7245824</WorkingSetSize>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1870	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1874	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1880	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 30 00 31 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>170112</QuotaPeakPagedPoolUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1994	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	1998	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2004	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 36 00 39 00 33 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>169320</QuotaPagedPoolUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2102	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2106	2	09 00		success or wait	3	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2112	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 32 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21232</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2236	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2240	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2246	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 30 00 39 00 36 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>20960</QuotaNonPagedPoolUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2354	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2358	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2364	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 31 00 36 00 30 00 39 00 37 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>1609728</PagefileUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2440	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2444	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2450	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 31 00 36 00 31 00 37 00 39 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1617920</PeakPagefileUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2542	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2546	2	09 00		success or wait	3	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2552	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 31 00 36 00 30 00 39 00 37 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>1609728</PrivateUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2624	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2628	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2632	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2678	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2682	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2686	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2716	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2720	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2726	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2766	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2770	2	09 00		success or wait	4	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2778	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2808	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2812	2	09 00		success or wait	4	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2820	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2890	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2894	2	09 00		success or wait	4	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2902	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2992	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	2996	2	09 00		success or wait	4	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3004	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 36 00 34 00 31 00 34 00 30 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4641406</Uptime>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3052	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3056	2	09 00		success or wait	4	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3064	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3154	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3218	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3276	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3366	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3370	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3380	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3454	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3458	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3468	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 32 00 30 00 38 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>62082</PageFaultCount>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3558	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 32 00 31 00 31 00 31 00 33 00 39 00 32 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121139200</PeakWorkingSetSize>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3672	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 32 00 30 00 37 00 37 00 30 00 35 00 36 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>120770560</WorkingSetSize>	success or wait	1	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3756	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3760	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3770	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 34 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 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>11406 08</QuotaPeakPagedPoolUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3886	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3890	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	3900	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 39 00 33 00 30 00 38 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 >1093088</ QuotaPagedPoolUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4000	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4004	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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 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>87 600</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4138	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4142	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.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 38 00 31 00 35 00 33 00 36 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>81536< /QuotaNonPagedPoolUsage>	success or wait	1	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4260	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4264	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4274	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 36 00 31 00 38 00 33 00 30 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>43618304</PagefileUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4352	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4356	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4366	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 38 00 35 00 30 00 36 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>45850624</PeakPagefileUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4460	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4464	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4474	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 36 00 31 00 38 00 33 00 30 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>43618304</PrivateUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4548	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4552	2	09 00		success or wait	4	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4560	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4606	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4610	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4616	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	2	6D29497A	unknown

Copyright Joe Security LLC 2023

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4666	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4698	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4702	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4704	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4752	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4790	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4794	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4798	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4850	4	0d 00 0a 00		success or wait	9	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4854	2	09 00		success or wait	18	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	4858	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 65 00 64 00 70 00 6d 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>edpm.exe</Parameter0>	success or wait	9	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	5512	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	5516	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	5518	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	5558	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	5562	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	5564	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	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	5602	4	0d 00 0a 00		success or wait	6	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	5606	2	09 00		success or wait	12	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	5610	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6164	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6168	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6170	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6210	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6214	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6216	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6254	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6258	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6262	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6356	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6360	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6364	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 64 00 70 00 64 00 71 00 68 00 63 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>dpdqhc, Inc.</SystemManufacturer>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6470	4	0d 00 0a 00		success or wait	1	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6474	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6478	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 64 00 70 00 64 00 71 00 68 00 63 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>dpdqhc7,1</SystemProductName>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6574	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6578	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6582	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6702	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6706	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6710	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 33 00 30 00 38 00 39 00 35 00 31 00 37 00 34 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>1630895174</OSInstallDate>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6792	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6796	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6800	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6902	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6906	2	09 00		success or wait	2	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6910	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6980	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6984	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	6986	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7026	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7030	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7032	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7066	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7070	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7074	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7176	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7212	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7216	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7218	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7242	4	0d 00 0a 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7246	2	09 00		success or wait	6	6D29497A	unknown

Copyright Joe Security LLC 2023

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7250	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7496	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7500	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7502	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7528	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7532	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7534	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 33 00 2d 00 30 00 32 00 2d 00 30 00 33 00 54 00 32 00 32 00 3a 00 31 00 37 00 3a 00 32 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-02-03T22:17:24Z">	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7634	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7638	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7642	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 34 00 36 00 38 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 33 00 30 00 31 00 35 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 33 00 30 00 31 00 35 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="304" PID="2468" UptimeMS="3015" TimeSinceCreationMS="3015" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7904	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7908	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7912	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	6D29497A	unknown

Copyright Joe Security LLC 2023

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7932	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7936	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7938	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7976	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7980	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	7982	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	8020	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	8024	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	8028	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 62 00 31 00 32 00 30 00 36 00 38 00 31 00 2d 00 62 00 62 00 39 00 39 00 2d 00 34 00 33 00 64 00 63 00 2d 00 38 00 39 00 34 00 61 00 2d 00 39 00 35 00 64 00 30 00 65 00 35 00 30 00 65 00 65 00 62 00 35 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>2b120681-bb99-43dc-894a-95d0e50eeb50</Guid>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	8126	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	8130	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	8134	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 33 00 2d 00 30 00 32 00 2d 00 30 00 33 00 54 00 32 00 32 00 3a 00 31 00 37 00 3a 00 32 00 34 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>2023-02-03T22:17:24Z</CreationTime>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	8232	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	8236	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	8238	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	8278	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD405.tmp.WERInternalMetadata.xml	8282	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	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD445.tmp.xml	0	4622	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_edpm.exe_98859aec2feace66336d4eb3ad62fedc1a5d529e_aad16012_04aefae6\Report.wer	0	2	fd fd		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_edpm.exe_98859aec2feace66336d4eb3ad62fedc1a5d529e_aad16012_04aefae6\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	168	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_edpm.exe_98859aec2feace66336d4eb3ad62fedc1a5d529e_aad16012_04aefae6\Report.wer	11250	48	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 31 00 36 00 33 00 34 00 31 00 31 00 35 00 32 00 38 00 32 00	MetadataHash=-1634115282	success or wait	1	6D29497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: edpm.exe PID: **5104**, Parent PID: **3528**

General

Target ID:	7
Start time:	23:17:29
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Roaming\ovawcpafrwk\edpm.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\ovawcpafrwk\edpm.exe" "C:\Users\user\AppData\Local\Temp\tchnhwrvi.exe" C:\Users\user\AppData\Loca
Imagebase:	0x1d0000
File size:	82432 bytes
MD5 hash:	64F982758878F6A97ED4B3D99CFBD371
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: **3692**, Parent PID: **5104**

General

Target ID:	9
Start time:	23:17:30
Start date:	03/02/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5104 -s 632
Imagebase:	0x980000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D2A1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC42.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC42.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_edpm.exe_98859aec2feace66336d4eb3ad62fedc1a5d529e_aad16012_0e2afae6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_edpm.exe_98859aec2feace66336d4eb3ad62fedc1a5d529e_aad16012_0e2afae6\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D29497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC42.tmp	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC42.tmp.xml	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC90.tmp.csv	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERED2D.tmp.txt	success or wait	1	6D29497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.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 fd 63 fd 05 12 00 00 00 00 00	MDMP c	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	6916	6	00 00 00 00 00 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.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 04 1b 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 13 00 00 fd fd fd 63 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 20 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 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	UBGenuineIntelWTc W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	8098	716	01 00 01 00 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 21 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 01 53 00 01 01 2b 00 02 01 2b 00 01 01 fd 66 71 74 17 04 00 fd 02 00 00 00 00 00 00 00 00 00 00 00 78 fd fd 00 78 fd fd 00 66 3c 1d 00 23 00 fd 77 16 02 00 00 4c fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	!!+S++fqtxxf<#wL+	success or wait	1	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	1620	168	fd 02 00 00 00 00 00 00 17 04 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 66 3c 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 1f 00 00	f<	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	10962	20	0e 00 00 00 fd 3b 1d 00 00 00 00 00 00 01 00 00 fd 2b 00 00	;+	success or wait	14	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	11190	256	30 fd fd fd 01 00 01 00 fd fd fd fd fd fd 49 fd fd fd fd fd fd fd 4d 0c fd fd fd fd fd fd 4d 10 fd fd fd fd fd fd fd fd fd fd fd fd 15 18 01 1e 00 6a 00 fd fd fd 15 1c 01 1e 00 fd fd fd fd fd fd 50 fd 15 20 01 1e 00 fd fd 75 10 fd fd 75 0c fd fd fd 74 07 53 fd 77 3d 00 00 59 fd 4d fd 5f 33 fd 5b fd 72 3d 00 00 fd cb fd 56 6a 01 fd 17 04 00 fd 56 6a 02 fd fd fd fd fd fd 0c 56 fd 15 08 01 1e 00 50 fd 15 0c 01 1e 00 5e cb fd 55 fd fd fd 35 fd 51 1e 00 fd 15 10 01 1e 00 fd fd 74 03 5d fd fd fd 75 18 fd 75 14 fd 75 10 fd 75 0c fd 75 08 fd fd fd fd fd 33 fd 50 50 50 50 50 fd fd fd fd fd fd fd 14 cb fd 55 fd fd 45 08 33 fd 3b 04 50 42 1e 00 74 13 41 fd fd 2d 72 fd 48 fd fd 11 77 0e 6a 0d 58 5d cb 04 54 42 1e 00 5d fd	0IMMjP uutSw=YM_3[r=VjVjVP^ U5Q t]uuuuu3PPPPPUE3;BtA-rHwjX]B]	success or wait	13	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	31410	4	fd fd 3d 01	=	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	8814	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 fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 00 fd fd fd 77 23 00 00 00 16 02 00 00 fd fd fd 00 2b 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	?+S++w#+	success or wait	3	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	1888	48	60 10 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 18 fd 3d 01 00 00 00 00 fd 02 00 00 fd 2c 00 00 fd 02 00 00 06 28 00 00	` =,(	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	1948	4	28 00 00 00	(	success or wait	40	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	6922	22	10 00 00 00 65 00 64 00 70 00 6d 00 2e 00 65 00 78 00 65 00 00 00	edpm.exe	success or wait	40	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	6164	752	00 00 fd 76 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 1f 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 fd fd 02 00 00 00 00 00 fd 01 03 00 00 00 00 c6 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 62 7f 03 00 00 00 00 2f fd 03 00 00 00 00 00 00 00 00 00 00 00 00 fd 16 1b 00 00 00 00 00 6f fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 32 06 00 00 00 00	v`A!-aBB?#@AZbb/o@2	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	31414	9022	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	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9EE.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 10 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 2a 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 18 00 00 0c fd 00 00 15 00 00 00 fd 01 00 00 fd 18 00 00 16 00 00 00 fd 00 00 00 6c 1a 00 00	*T8Tl	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 31 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5104</Pid>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 64 00 70 00 6d 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>edpm.exe</ImageName>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1072	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1170	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 33 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2038</Uptime>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1212	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1216	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1220	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1302	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1306	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1310	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1362	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1366	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1370	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1414	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1418	2	09 00		success or wait	3	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1424	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 38 00 38 00 39 00 37 00 33 00 33 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>8897312</PeakVirtualSize>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1510	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1514	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1520	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 38 00 37 00 37 00 39 00 37 00 37 00 36 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>87797760</VirtualSize>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1590	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1594	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1600	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 37 00 36 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1766</PageFaultCount>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1674	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1678	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1684	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 38 00 36 00 34 00 38 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>6864896</PeakWorkingSetSize>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1780	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1784	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1790	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 38 00 36 00 34 00 38 00 39 00 36 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>6864896</WorkingSetSize>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1870	4	0d 00 0a 00		success or wait	1	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1874	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1880	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 36 00 38 00 38 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>168856</QuotaPeakPagedPoolUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1994	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	1998	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2004	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 36 00 38 00 32 00 38 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>168288</QuotaPagedPoolUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2102	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2106	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2112	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 30 00 38 00 34 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>20840</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2236	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2240	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2246	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 30 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>20568</QuotaNonPagedPoolUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2354	4	0d 00 0a 00		success or wait	1	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2358	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2364	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 31 00 35 00 36 00 38 00 37 00 36 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>1568768</PagefileUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2440	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2444	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2450	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 31 00 35 00 37 00 36 00 39 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1576960</PeakPagefileUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2542	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2546	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2552	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 31 00 35 00 36 00 38 00 37 00 36 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>1568768</PrivateUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2624	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2628	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2632	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2678	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2682	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2686	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2716	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2720	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2726	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	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2766	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2770	2	09 00		success or wait	4	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2778	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2808	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2812	2	09 00		success or wait	4	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2820	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2890	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2894	2	09 00		success or wait	4	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2902	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2992	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	2996	2	09 00		success or wait	4	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3004	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 36 00 34 00 37 00 35 00 35 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4647557</Uptime>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3052	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3056	2	09 00		success or wait	4	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3064	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3154	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3218	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3276	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3366	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3370	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3380	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3454	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3458	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3468	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 32 00 33 00 33 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>62330</PageFaultCount>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3558	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 32 00 31 00 31 00 33 00 39 00 32 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121139200</PeakWorkingSetSize>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3672	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 35 00 32 00 33 00 32 00 37 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>115232768</WorkingSetSize>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3756	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3760	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3770	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 34 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 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>1140608</QuotaPeakPagedPoolUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3886	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3890	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	3900	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 39 00 38 00 38 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>1089888</QuotaPagedPoolUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4000	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4004	2	09 00		success or wait	5	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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 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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4138	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4142	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.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 38 00 31 00 35 00 33 00 36 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>81536</QuotaNonPagedPoolUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4260	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4264	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4274	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 33 00 38 00 34 00 35 00 37 00 33 00 34 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>38457344</PagefileUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4352	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4356	2	09 00		success or wait	5	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4366	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 38 00 35 00 30 00 36 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>45850624</PeakPagefileUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4460	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4464	2	09 00		success or wait	5	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4474	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 33 00 38 00 34 00 35 00 37 00 33 00 34 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>38457344</PrivateUsage>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4548	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4552	2	09 00		success or wait	4	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4560	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4606	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4610	2	09 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4616	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4666	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4698	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4702	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4704	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4752	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4790	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4794	2	09 00		success or wait	2	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4798	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4850	4	0d 00 0a 00		success or wait	9	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4854	2	09 00		success or wait	18	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	4858	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 65 00 64 00 70 00 6d 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>edpm.exe</Parameter0>	success or wait	9	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	5512	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	5516	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	5518	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	5558	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	5562	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	5564	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	5602	4	0d 00 0a 00		success or wait	6	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	5606	2	09 00		success or wait	12	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	5610	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6164	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6168	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6170	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6210	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6214	2	09 00		success or wait	1	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6216	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6254	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6258	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6262	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6356	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6360	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6364	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 64 00 70 00 64 00 71 00 68 00 63 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>dpdqhc, Inc.</SystemManufacturer>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6470	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6474	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6478	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 64 00 70 00 64 00 71 00 68 00 63 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>dpdqhc7,1</SystemProductName>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6574	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6578	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6582	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	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6702	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6706	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6710	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 33 00 30 00 38 00 39 00 35 00 31 00 37 00 34 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>1630895174</OSInstallDate>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6792	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6796	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6800	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6902	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6906	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6910	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6980	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6984	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	6986	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7026	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7030	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7032	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7066	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7070	2	09 00		success or wait	2	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7074	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7176	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7212	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7216	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7218	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7242	4	0d 00 0a 00		success or wait	3	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7246	2	09 00		success or wait	6	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7250	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7494	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7498	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7500	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7526	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7530	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7532	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 33 00 2d 00 30 00 32 00 2d 00 30 00 33 00 54 00 32 00 32 00 3a 00 31 00 37 00 3a 00 33 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-02-03T22:17:31Z">	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7632	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7636	2	09 00		success or wait	2	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7640	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 31 00 30 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 39 00 33 00 37 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 33 00 37 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="309" PID="5104" UptimeMS="937" TimeSinceCreationMS="937" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7898	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7902	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7906	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7926	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7930	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7932	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7970	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7974	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	7976	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	8014	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	8018	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	8022	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 31 00 35 00 63 00 37 00 32 00 33 00 33 00 2d 00 36 00 34 00 65 00 33 00 2d 00 34 00 38 00 30 00 32 00 2d 00 62 00 64 00 38 00 34 00 2d 00 64 00 61 00 38 00 35 00 37 00 31 00 30 00 36 00 62 00 32 00 33 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>815c7233-64e3-4802-bd84-da857106b23b</Guid>	success or wait	1	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	8120	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	8124	2	09 00		success or wait	2	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	8128	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 33 00 2d 00 30 00 32 00 2d 00 30 00 33 00 54 00 32 00 32 00 3a 00 31 00 37 00 3a 00 33 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>2023-02-03T22:17:31Z</CreationTime>	success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	8226	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	8230	2	09 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	8232	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	8272	4	0d 00 0a 00		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC12.tmp.WERInternalMetadata.xml	8276	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC42.tmp.xml	0	4622	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	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_edpm.exe_98859aec2feace66336d4eb3ad62fedc1a5d529e_aad16012_0e2afae6\Report.wer	0	2	fd fd		success or wait	1	6D29497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_edpm.exe_98859aec2feace66336d4eb3ad62fedc1a5d529e_aad16012_0e2afae6\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	167	6D29497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_edpm.exe_98859aec2feace66336d4eb3ad62fedc1a5d529e_aad16012_0e2afae6\Report.wer	11152	48	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 31 00 39 00 31 00 36 00 35 00 35 00 37 00 35 00 32 00 34 00	MetadataHash=-1916557524	success or wait	1	6D29497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Disassembly

No disassembly