ID: 795634
Sample Name:
fyTwP4SHWF.exe
Cookbook: default.jbs
Time: 05:13:13
Date: 01/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Windows Analysis Report

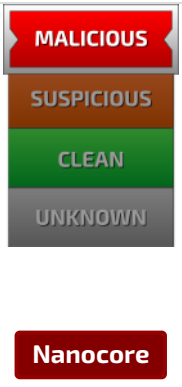
fyTwP4SHWF.exe

Overview

General Information

Sample Name:	fyTwP4SHWF.exe
Analysis ID:	795634
MD5:	d3e933b0aab5…
SHA1:	ee600eacf16a1..
SHA256:	51ab5d042dee…
Tags:	32 exe trojan
Infos:	

Detection



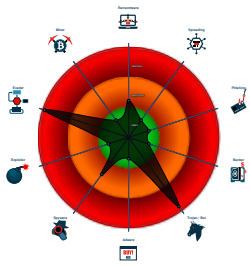
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Yara detected Nanocore RAT
- 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**
- fyTwP4SHWF.exe (PID: 6032 cmdline: C:\Users\user\Desktop\fyTwP4SHWF.exe MD5: D3E933B0AAB571BDC73355A106D657E0)
  - rnixgfly.exe (PID: 4904 cmdline: "C:\Users\user~1\AppData\Local\Temp\rnixgfly.exe" C:\Users\user~1\AppData\Local\Temp\somvwkehjlp.rt MD5: C1DC97853E14C21B463C6E95B21C300C)
    - rnixgfly.exe (PID: 3192 cmdline: C:\Users\user~1\AppData\Local\Temp\rnixgfly.exe MD5: C1DC97853E14C21B463C6E95B21C300C)
- jfcarlsrvb.exe (PID: 4528 cmdline: "C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe" "C:\Users\user~1\AppData\Local\Temp\rnixgfly.exe" C:\Users\user~1\ MD5: C1DC97853E14C21B463C6E95B21C300C)
  - WerFault.exe (PID: 4388 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4528 -s 656 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- jfcarlsrvb.exe (PID: 5880 cmdline: "C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe" "C:\Users\user~1\AppData\Local\Temp\rnixgfly.exe" C:\Users\user~1\ MD5: C1DC97853E14C21B463C6E95B21C300C)
  - WerFault.exe (PID: 5912 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5880 -s 628 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "7dcf7c5d-e4be-40f9-826b-505d4386",
  "Group": "Inflows",
  "Domain1": "boele.duckdns.org",
  "Domain2": "boele.duckdns.org",
  "Port": 6269,
  "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
00000002.00000002.508686978.00000000067C0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x16e3:$x1: NanoCore.ClientPluginHost • 0x171c:$x2: IClientNetworkHost
00000002.00000002.508686978.00000000067C0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x16e3:$x2: NanoCore.ClientPluginHost • 0x1800:$s4: PipeCreated • 0x16fd:$s5: IClientLoggingHost
00000002.00000002.508686978.00000000067C0000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x175f:$x2: NanoCore.ClientPlugin • 0x16e3:$x3: NanoCore.ClientPluginHost • 0x1775:$i3: IClientNetwork • 0x16fd:$i6: IClientLoggingHost • 0x171c:$i7: IClientNetworkHost • 0x1491:$s1: ClientPlugin • 0x1768:$s1: ClientPlugin
00000002.00000002.508686978.00000000067C0000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x16e3:$a1: NanoCore.ClientPluginHost • 0x175f:$a2: NanoCore.ClientPlugin • 0x16fd:$b9: IClientLoggingHost
00000002.00000002.509009346.0000000006860000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
Click to see the 97 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.rnixgfly.exe.2223658.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
1.2.rnixgfly.exe.2223658.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
1.2.rnixgfly.exe.2223658.2.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
1.2.rnixgfly.exe.2223658.2.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected
1.2.rnixgfly.exe.2223658.2.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 294 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: 192.168.2.7 - Destination IP: 45.137.65.132 −

Timestamp:	192.168.2.745.137.65.132497346269281676 6 02/01/23-05:15:28.676401
SID:	2816766

Source Port:	49734
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.7	
Timestamp:	45.137.65.132192.168.2.76269497272841753 02/01/23-05:14:56.574585
SID:	2841753
Source Port:	6269
Destination Port:	49727
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.7	
Timestamp:	45.137.65.132192.168.2.76269497442841753 02/01/23-05:16:22.394490
SID:	2841753
Source Port:	6269
Destination Port:	49744
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.745.137.65.1324972862692816766 02/01/23-05:15:03.576741
SID:	2816766
Source Port:	49728
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.745.137.65.1324971162692816766 02/01/23-05:14:19.296579
SID:	2816766
Source Port:	49711
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 3 - Source IP: 45.137.65.132 - Destination IP: 192.168.2.7	
Timestamp:	45.137.65.132192.168.2.76269497402810451 02/01/23-05:15:57.113635
SID:	2810451
Source Port:	6269
Destination Port:	49740
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.7	
Timestamp:	45.137.65.132192.168.2.76269497222841753 02/01/23-05:14:40.350682
SID:	2841753
Source Port:	6269
Destination Port:	49722
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.745.137.65.1324972062692816766 02/01/23-05:14:35.257700
SID:	2816766
Source Port:	49720
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.7	
Timestamp:	45.137.65.132192.168.2.76269497402841753 02/01/23-05:15:57.113635
SID:	2841753
Source Port:	6269
Destination Port:	49740
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.745.137.65.1324973062692816766 02/01/23-05:15:09.580115
SID:	2816766
Source Port:	49730
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.745.137.65.1324973362692816766 02/01/23-05:15:22.661130
SID:	2816766
Source Port:	49733
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.7	
Timestamp:	45.137.65.132192.168.2.76269497232841753 02/01/23-05:14:46.707897
SID:	2841753
Source Port:	6269
Destination Port:	49723
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.7	
Timestamp:	45.137.65.132192.168.2.76269497242841753 02/01/23-05:14:51.698320
SID:	2841753
Source Port:	6269
Destination Port:	49724
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.7	
Timestamp:	45.137.65.132192.168.2.76269497412841753 02/01/23-05:16:02.171075
SID:	2841753
Source Port:	6269
Destination Port:	49741
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.7	
Timestamp:	45.137.65.132192.168.2.76269497432841753 02/01/23-05:16:07.296877
SID:	2841753
Source Port:	6269
Destination Port:	49743
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 45.137.65.132 - Destination IP: 192.168.2.7	
Timestamp:	45.137.65.132192.168.2.76269497142810290 02/01/23-05:14:28.429351
SID:	2810290
Source Port:	6269

Destination Port:	49714
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.745.137.65.132497376269281676 6 02/01/23-05:15:41.799633
SID:	2816766
Source Port:	49737
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.745.137.65.132497416269281676 6 02/01/23-05:16:02.177770
SID:	2816766
Source Port:	49741
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.7	
Timestamp:	45.137.65.132192.168.2.76269497392841753 02/01/23-05:15:52.038941
SID:	2841753
Source Port:	6269
Destination Port:	49739
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.7 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.745.137.65.132497146269281676 6 02/01/23-05:14:29.178500
SID:	2816766
Source Port:	49714
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.7	
Timestamp:	45.137.65.132192.168.2.76269497312841753 02/01/23-05:15:14.788888
SID:	2841753
Source Port:	6269
Destination Port:	49731
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.7	
Timestamp:	45.137.65.132192.168.2.76269497352841753 02/01/23-05:15:33.801145
SID:	2841753
Source Port:	6269
Destination Port:	49735
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.7	
Timestamp:	45.137.65.132192.168.2.76269497382841753 02/01/23-05:15:46.943033
SID:	2841753
Source Port:	6269
Destination Port:	49738
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

Yara detected Nanocore RAT

Compliance

Detected unpacking (overwrites its own PE header)

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

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

.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

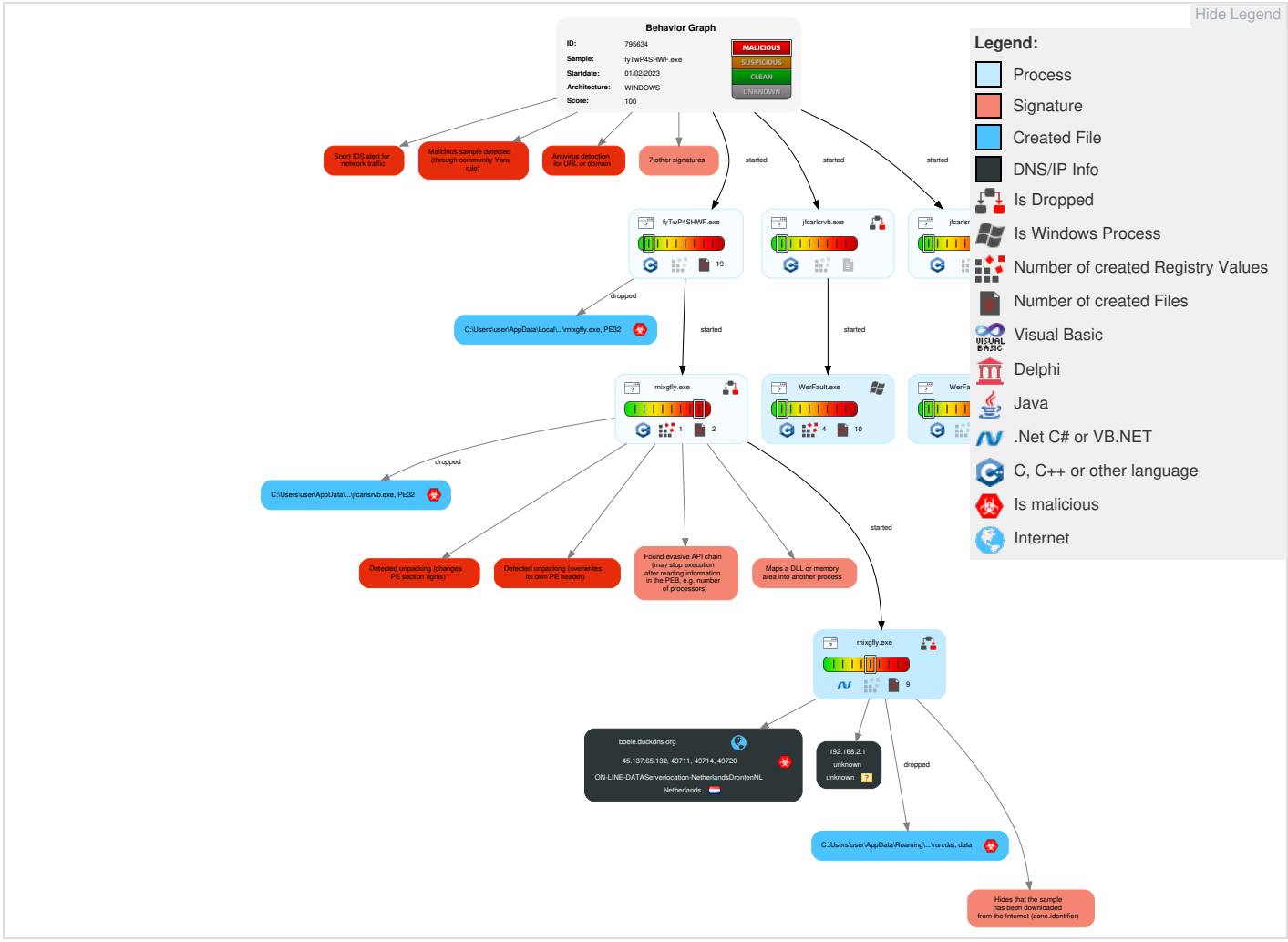
Detected Nanocore Rat

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	1 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	1 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)	3 1 Software Packing	NTDS	4 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
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

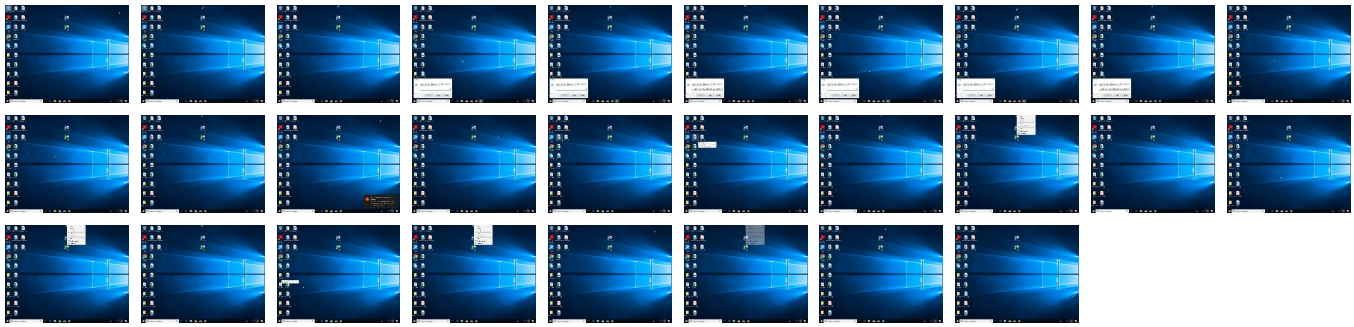
Behavior Graph



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
fyTwP4SHWF.exe	51%	ReversingLabs	Win32.Trojan.Nemesis	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\rnixgfly.exe	10%	ReversingLabs	Win32.Trojan.InjectorX	
C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe	10%	ReversingLabs	Win32.Trojan.InjectorX	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rnixgfly.exe.4f60000.20.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.rnixgfly.exe.ba0000.1.unpack	100%	Avira	HEUR/AGEN.1230506		Download File
2.2.rnixgfly.exe.58c0000.24.unpack	100%	Avira	TR/NanoCore.fadte		Download File
2.2.rnixgfly.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.fyTwP4SHWF.exe.291d7ec.1.unpack	100%	Avira	HEUR/AGEN.1230498		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
boele.duckdns.org	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
boele.duckdns.org	45.137.65.132	true	true		unknown

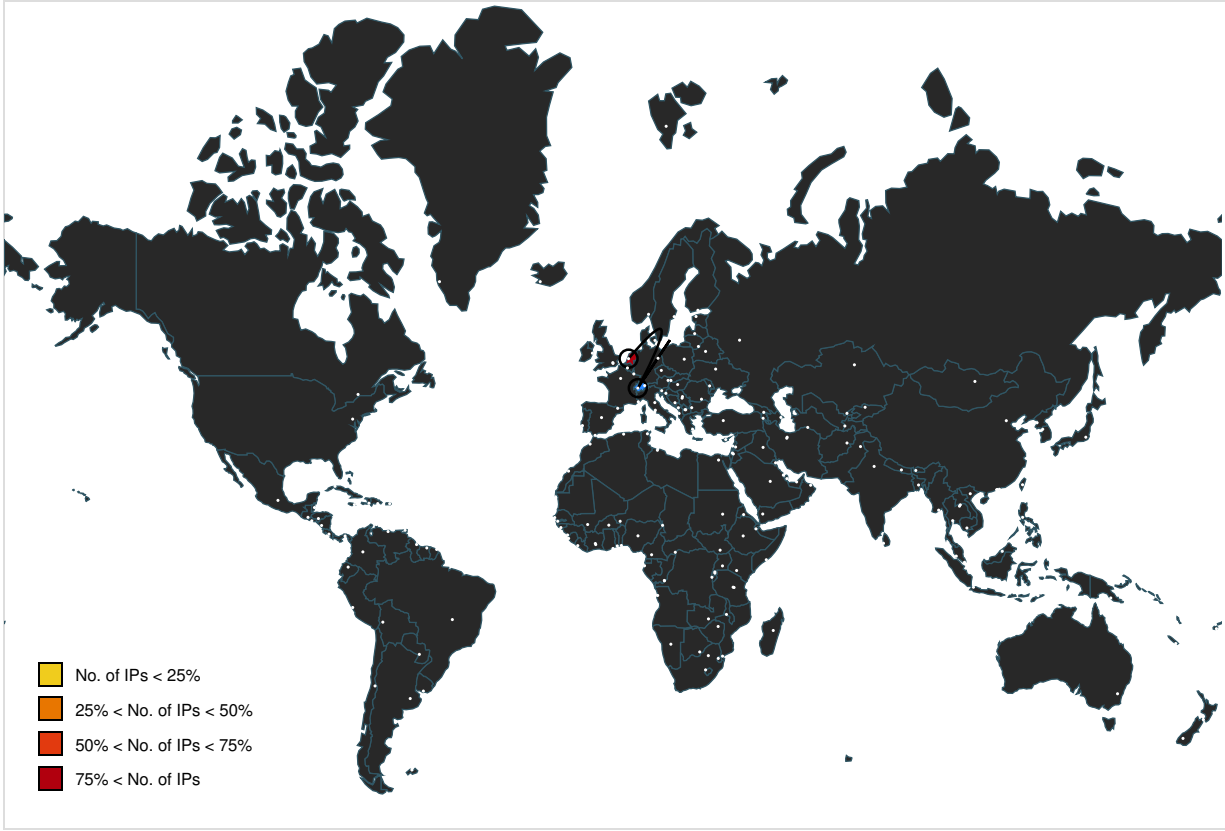
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
boele.duckdns.org	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	fyTwP4SHWF.exe	false		high
http://google.com	rnixgfly.exe, 00000002.00000002.50394157 0.000000000366D000.00000004.00000800.000 20000.00000000.sdmp, rnixgfly.exe, 00000 002.00000002.508870070.0000000006820000. 00000004.08000000.00040000.00000000.sdmp, rnixgfly.exe, 00000002.00000002.503941570.000000 0003851000.00000004.00000800.00020000.00 000000.sdmp, rnixgfly.exe, 00000002.0000 0002.502791120.00000000025CF000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	rnixgfly.exe, 00000002.00000002.50279112 0.0000000002551000.00000004.00000800.000 20000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.137.65.132	boele.duckdns.org	Netherlands		204601	ON-LINE-DATAServerlocation-NetherlandsDrontenNL	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	795634
Start date and time:	2023-02-01 05:13:13 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 18s
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:	19
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:	fyTwP4SHWF.exe

Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/17@20/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 86.6% (good quality ratio 82.8%) • Quality average: 82.2% • Quality standard deviation: 26.6%
HCA Information:	• Successful, ratio: 99% • 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, WerFault.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.21, 104.208.16.94
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus16.westus.cloudapp.azure.com, ctldl.windowsupdate.com, watson.telemetry.microsoft.com, onedsblobprdcus16.centralus.cloudapp.azure.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.
- VT rate limit hit for: fyTwP4SHWF.exe

Simulations

Behavior and APIs

Time	Type	Description
05:14:12	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run ryhcwrfexidnfv C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe "C:\Users\user~1\AppData\Local\Temp\rnixgfly.exe" C:\Users\user~1\
05:14:16	API Interceptor	938x Sleep call for process: rnixgfly.exe modified
05:14:21	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run ryhcwrfexidnfv C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe "C:\Users\user~1\AppData\Local\Temp\rnixgfly.exe" C:\Users\user~1\
05:14:31	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_jfcarlsrvb.exe_f36b28a8e4f7e8b0d66d5d37aab64913222e2789_70c0d770_117b1399\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):	0.9282124186735965
Encrypted:	false
SSDEEP:	96:voIuFSZJXdwhja72TNFpXlQcQ4c6K/cEIcw3RGxD+HbHg/LAeugtYsaGFYAKcEoi:ANuZKHWoyF7joqAt/u7sIS274Ith
MD5:	DDF46C9A2DDD07C0336B3027C3EA945A
SHA1:	AEDDE88C7A40C1949C6FEFAF9BB5E7B4CA2EEFFB
SHA-256:	A099199692B0F30C4A6D330C46C9008E331B1AC06D2A462A7799E4937F487408
SHA-512:	7582EBA198370AF8094B62DCE81FE03B20010A17F11D06A291ED2D749D495462C43B9A9F027AEB9A88D265100A62AE86745740CA91AFD7A788616EF8D6D4A23
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.=.1.3.3.1.9.7.3.0.8.6.7.5.0.2.7.7.4.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.1.9.7.3.0.8.6.8.4.5.5.8.9.7.3.....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.=.6.3.f.9.2.d.a.3.-.b.5.b.5.-.4.c.d.8.-.a.6.7.d.-.1.9.9.6.4.e.e.f.4.b.c.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.1.c.4.0.7.3.0.-.0.7.e.b.-.4.9.7.5.-.9.6.0.c.-.8.9.5.0.d.3.2.f.5.d.d.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.=.j.f.c.a.r.l.s.r.v.b...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.1.b.0.-.0.0.0.1.-.0.0.1.a.-.7.2.e.a.-.c.4.1.8.3.f.3.6.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.f.7.7.7.8.6.6.2.5.d.3.b.5.3.a.d.8.2.2.b.5.3.0.5.4.3.a.d.6.1.1.0.0.0.0.f.f.f.f.!.0.0.0.0.7.8.a.d.b.b.8.a.1.e.f.c.b.4.f.0.a.b.5.b.e.b.a.8.a.3.c.f.7.0.e.5.0.7.4.b.e.9.4.5.!.j.f.c.a.r.l.s.r.v.b...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_jfcarlsrvb.exe_f36b28a8e4f7e8b0d66d5d37aab64913222e2789_70c0d770_17471e38\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):	0.9211945957633184
Encrypted:	false
SSDEEP:	96:nMF+JX9whja72TNFpXlQcQ4c6K/cEIcw3RGxD+HbHgA5aeugtYsaoDtsEa2bm6oU:MgZqHWoyF7jEhy8/u7sIS274Ith
MD5:	B1B32A4B231CEA5577B2396F64E8DED7
SHA1:	D4FF3D70716DAF5B81E34199EE3D8697379AB5EF
SHA-256:	FC8D6BC42D8EDB5246BFB340ABD975F0AD3328D22D5283B8108A09CCCF91E8C9
SHA-512:	1DDCC810636F2EDF6984C08AE2AA96A3F017CD0C70A15B829279FE1A5985BCAD43CBB4C47E3EC08AD46C70F02C450CFC1E7987894A1A76241B24595D09C629AF
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.=.1.3.3.1.9.7.3.0.8.7.2.0.4.3.7.9.0.8.....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.=.1.3.3.1.9.7.3.0.8.7.3.4.5.0.3.1.7.1.....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.=.c.f.4.9.2.b.d.5.-.1.2.3.2.-.4.0.a.0.-.a.9.5.3.-.e.e.c.2.c.4.c.f.3.f.1.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.3.7.b.7.b.b.a.-.8.7.3.c.-.4.8.b.d.-.8.d.4.b.-.7.7.a.f.4.2.6.8.b.d.6.0.....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.=.j.f.c.a.r.l.s.r.v.b...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.f.8.-.0.0.0.1.-.0.0.1.a.-.1.4.6.3.-.3.f.1.e.3.f.3.6.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.f.7.7.7.8.6.6.2.5.d.3.b.5.3.a.d.8.2.2.b.5.3.0.5.4.3.a.d.6.1.1.0.0.0.0.f.f.f.f.!.0.0.0.0.7.8.a.d.b.b.8.a.1.e.f.c.b.4.f.0.a.b.5.b.e.b.a.8.a.3.c.f.7.0.e.5.0.7.4.b.e.9.4.5.!.j.f.c.a.r.l.s.r.v.b...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 1 13:14:32 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	38214
Entropy (8bit):	2.1593548134413028
Encrypted:	false
SSDEEP:	192:p6wEptF2xdgXDOG4RCqujP/S0xp2yEDruvXVqDNn:UWuX6GsgS8XvXm
MD5:	80F8852BF24981FB18C0A96C052A2B7F
SHA1:	16D60E79EA4971593403FD2EE5F607EE6BE87A34
SHA-256:	DE8579536E029CC7652EDAD3AACF068A191165F3E6A1F6AB4E6D76FE9E448F8C
SHA-512:	CC17FC6E4399C114EDE115243F9C8BF49997E29CF87D7BF6D36A2D06FB7E9BCDC8E043849BAD2303474B64AC6B7FDD69D70E991FDB19743B18F8030841D2959
Malicious:	false

Reputation:	low
Preview:	MDMP..... .....e.c.....(.....^,.....T.....8.....T.....6|.....U.....B.....H.....GenuineIntelW.....T.....e.c..... .....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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):	8350
Entropy (8bit):	3.690202005811949
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi5+6l9h6YApSUSAgmf0SQCpr789bE/sfVsm:RrlsNiw66h6YuSUSAgmf0SkEkfL
MD5:	88780EF5D141127E1DFEF0794FC4D422
SHA1:	25C0D6C64EA99F73330E819125FE96D2F0CA049C
SHA-256:	D043A2505305FFAFC024623E94C00ADFDDC9379F383544450A07BD92D3268884
SHA-512:	DE207DBA4CC31E054D5F7963F3FAD6024458D3F016594AB87EDC65A42AA97BA09E4F8BFC7AA91D2E83EC53B592A32917C5260CB22D5AE56C733034AC05E8D544
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.>.5.8.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER17A2.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4664
Entropy (8bit):	4.424392328941231
Encrypted:	false
SSDEEP:	48:cvIwSD8zsRJgtWI97TWgc8sqYjy68fm8M4JczIFA+q8vczhusvypV+d:uITfj8igrsqYuPJ6xK6hus6P+d
MD5:	AF14FA1090319F74BF2092FCFD6F5C79
SHA1:	1B87280B0A5F4D634A8B691FE3EC21856168AEDA
SHA-256:	791A72355185A77E4F49F6E60C0FF995E65244D7246C9037E5AED5C9B23F71F5
SHA-512:	BFF3B31ED93183211A0B999FA65B9A773E1CBFD29B110103FB2C73E185C7BC6C58D07A10C184EE36378803259F386329BA960B232DF5B88C9C95327B2120A2C
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="1893505" />.. <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\WER31E.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 1 13:14:27 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	38630
Entropy (8bit):	2.1542418285429483
Encrypted:	false
SSDEEP:	192:uaVJF1NTbMK4SvwOX4UElZAxEsbybEg20xpGPDD0gfTw6DqnHYD:VPMKfXJEgyse2xRfTw6YY
MD5:	CA6B0C408F1446644DB673F890264054
SHA1:	106089C73F0B60231EAC2C863703834C5D1F243C
SHA-256:	DE57C4FFE0354AA56F93146AD380A89195BEF29447F1F01A4D37A27076E21C4D
SHA-512:	2DCFDE5A0938C2D76E582A28FD43AC463145D6447A7BCDAFAF0442F676AADB811DD4B26267A56A78A9FFE559EEB54EAE77943BE33D948F017BC193F9F2DD3BB8
Malicious:	false

Reputation:	low
Preview:	MDMP..... .....e.c.....,.....T.....8.....T.....(....|.....0.....U.....B.....GenuineIntelW.....T.....e.c..... .....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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):	8356
Entropy (8bit):	3.691371045380274
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/f6oe6YATSU2kNgmf0SQCprh89bvOsfylm:RrlsNiX6h6YkSU2Egmf0SWvNf5
MD5:	BFA45D9D415A6E65115D148151951505
SHA1:	9D203365D8B26D118F7F9FAA04A32309D25915A8
SHA-256:	E0276D450652BEC9F95144EBF39D7E2BC613BCC12443F5510E14548B7B228E6A
SHA-512:	5B70D83C5A91C0DF4FEA3FD8BB4322D56BB692257DF4C13DC14C435841085F0C037A9AC1D98B624497A98FC83999F3E9AA20BFF86C15EB4F41E92FEF3F7145E
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.>.4.5.2.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A1.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4664
Entropy (8bit):	4.424419638363648
Encrypted:	false
SSDEEP:	48:cvIwSD8zsRJgtWI97TWgc8sqYju8fm8M4JczIFjg+q8vczD+usvypVDd:uITfj8igrsqY/J6xK6Cus6PDd
MD5:	39F1047F409235BC85CCC6B8A5FD5470
SHA1:	9873EA4CCA3B6151E1492A3F4C6299D5610E9FC6
SHA-256:	B4FBD8A971C0251505D10F2DFD639DC9ED36E044904B7B632169E5CFDD41C723
SHA-512:	4367384E07D518E5C89F8FEA3BD67E4A9B8182B5427461DD19876F068BFCFFFF11B0C8D88FD6A4BB407580790AAB6D0125E3DBA8D0BE35F3D609C1D5C121374
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="1893505" />.. <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\nsvBAAC.tmp

Process:	C:\Users\user\Desktop\fyTwP4SHWF.exe
File Type:	data
Category:	dropped
Size (bytes):	406476
Entropy (8bit):	7.760217782520545
Encrypted:	false
SSDEEP:	12288:DfIs4bcdUHKgcuzRlCDlNXhJGjvwDjpzxTSmFTo:DfIhcdUD1lC7hJGs5xTjBo
MD5:	306A577A34A568DC94A31C8EB371E05A
SHA1:	5EA8978456D1F1198C9C806F9435DA09EA943555
SHA-256:	50F3AC3A1EBC8EC50D101E815DDB00A1DE7284D85C5502E7569C3BC7BCF91F25
SHA-512:	0E9A2A2228694DC61F206BD8897C645FF8E76B635ECC22AF5262C2196E13D32CBDEDFF6BDF26637BD3BF8D387C6556A78781828E4390B2C29973040B17A376B
Malicious:	false

Reputation:	low
Preview:	&6.....,.....y...0'.....@5.....6..... .....G.....j.....9..... ....

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

Process:	C:\Users\user\Desktop\fyTwP4SHWF.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	76800
Entropy (8bit):	6.349678040473841
Encrypted:	false
SSDEEP:	1536:v/9cI7eE+7q3xJ6qI8ZZ9kmQFo4EFFWD3gjn5LIPU4l3:v/9cIWcxTZ3km34EFkOX4l3
MD5:	C1DC97853E14C21B463C6E95B21C300C
SHA1:	78ADBB8A1EFCB4F0AB5BEBA8A3CF70E5074BE945
SHA-256:	F18C6867F028E0E31A939FDB580762F57DCD11BB25B11E632EE22F21203DCC31
SHA-512:	04DFC132DBC5D31EBEA2E8453F065E2FCB67224F60A0EB0F53C27CBA6A36208A915E14B8E877F92C5FBA5C583580EBF759BFC650D7B95A526E4703A71F700A2B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Oe8%..Vv..Vv..Vvdr.v+.Vvdr.v..Vv.|.v..Vv..Wv..Vvdr.v|.Vvdr.v..VvRich..Vv.....PE..L.....c.....v.....3.....@.....#..... .....text...J..... ..`.rdata...1.....2.....@..@.data....B...@.....@..... ....

C:\Users\user\AppData\Local\Temp\somvwkehjlp.rt

Process:	C:\Users\user\Desktop\fyTwP4SHWF.exe
File Type:	data
Category:	dropped
Size (bytes):	7840
Entropy (8bit):	7.191226445255042
Encrypted:	false
SSDEEP:	192:darcitQvArWiPvECb9l5E3JHuQOoLHqGDcfumovUX7fN+:uCYrNPvEEzOjnKRmdsLN+
MD5:	E3C9D191E461DB735E4FDF1AC0FD72A5
SHA1:	0E8F30B10F46933786D4525F59D4ABEA09D519FC
SHA-256:	20838738B10F16E37211678286DBE6E5561E0057770344D5C9BF9F6865FC217D
SHA-512:	C04EE58FFC5ACCEFBE16F5F36281348E1D536E8E47105CF7A70D67FE93ED4A517FE164F960EFFF45A43EE40D5453A63D176E8FE44928D12AD469A0C043A935A2
Malicious:	false
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.[WlT.}....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.lT.}._\hR.t...R.}.^.y.W.y.R.u.....ZR..Jo....\5$.O

C:\Users\user\AppData\Local\Temp\vvnwaf.f

Process:	C:\Users\user\Desktop\fyTwP4SHWF.exe
File Type:	data
Category:	dropped
Size (bytes):	307958
Entropy (8bit):	7.98837190566036
Encrypted:	false
SSDEEP:	6144:hApS0PxPJG0RbcXNuGiHKgagwuzHEElCDlN5yObFhM4Gj0cwzRFE:hfIs4bcdUHKgcuzRlCDlNXhJGjvwDE
MD5:	FC0382D6DBF66C328188C64CACD86ED6
SHA1:	F7AF5088065FD1F9B66D8F4EE4041E3B8430CC33
SHA-256:	60C585E63B9378D1ED35E059B6BC6CC362129A4BFD40F70B0037724C1540AA54
SHA-512:	300D0BB1FBA8E4CE455C9B0AF121A247FA94A3DDE5D37339FC6CCA1DCB52D568C6EAD0CEA6484A26C574AE03059ADCF2FF24BC4C114ADF54EE10DA1874664B2A
Malicious:	false

Preview:	Cs...w.W7.3.=Q.....4....L".O..$J{..{.....#..+.E..4...Y...6.).P.8...^.....Y..M..m.v.4AI..*.p.8..i.M5.Z-u..q..".G.>..wq...D...v.!W.bX..+..f.....>#uRS>.~3.$Oty.}.WeL.].t..o...Y .F.S.F..G..k...g...."...S..S....$.....4h.....h.."...'.C.q..i.w..:.3....1...4....L".O.0.q.r.....>#..1.E..4..~.@.X).7u..|1....]..k.....p..A.z.1.KAu...y{aS4.P....M.U.G.T>..R..e.]ho.[....{.7.N ..PMY}_.s.....U@.....d>.8...>5o....e..lh.V.v.%...'..Os....?./..s.?.=.b4.KLc<.....n."QX.Cn."...'.C..../.w...3ZxQ..]......L".O..$J{.C{..Sj.g.R..{.#....E.4...Y....X)i7u..|1.....$`.....E .....zU1.!..`..y{wS4.P.K.MP..B.>....e..\.h.*....r{...N+..MY}_.B..q..U@.....d>.8..a..5y....e..lh.V.v.%...'..Os....Du|..s.?.=.b4.KLcg.....n."QX.Cn."...'.C.q..i.w..7.3Z`Q.....4.. ..L".O..$J{..{.....#..+.E..4..~Y....X)i7u..|1.....]..k.....A.z.1.!Au`..y{wS4.P...M.U.G.>..R..e.]h.2....{...N+..MY}_.s.....U@.....d>.8..a..5y....e..lh.V.v.%...'..Os....Du|..s.?.=.b4. KLcg.....

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

Process:	C:\Users\user\AppData\Local\Temp\rnixgfly.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\rnixgfly.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:1:1
MD5:	CBBA5F74CCE62678ECC52D978F037A9F
SHA1:	3E39F355F2478AF39A83DC12068D7CC036474234
SHA-256:	D06D749AA9BC3D4B78BC0FDFA28C3FD74A87EEFD94A59362437FC1FE68184B9E
SHA-512:	1E380CE236852AC82606848C60D3B3DC8D2859DBC476C7692B983102BF8AF8B93D87D58B7DA1C81937ABDBB51DAC567DB192CCCA6BC852C6A4D2628FD3B31 00
Malicious:	**true**
Preview:	..=8V..H

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

Process:	C:\Users\user\AppData\Local\Temp\rnixgfly.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:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44 F8
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\rnixgfly.exe
File Type:	data
Category:	dropped
Size (bytes):	327432

Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm: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\ilkqegcy\jfcarlsrvb.exe

Process:	C:\Users\user\AppData\Local\Temp\rnixgfly.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	76800
Entropy (8bit):	6.349678040473841
Encrypted:	false
SSDEEP:	1536:v/9cl7eE+7q3xJ6ql8ZZ9kmQFo4EFFWD3gjn5LIPU4l3:v/9clWcxTZ3km34EFkOX4l3
MD5:	C1DC97853E14C21B463C6E95B21C300C
SHA1:	78ADBB8A1EFCB4F0AB5BEBA8A3CF70E5074BE945
SHA-256:	F18C6867F028E0E31A939FDB580762F57DCD11BB25B11E632EE22F21203DCC31
SHA-512:	04DFC132DBC5D31EBEA2E8453F065E2FCB67224F60A0EB0F53C27CBA6A36208A915E14B8E877F92C5FBA5C583580EBF759BFC650D7B95A526E4703A71F700A2B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Oe8%..Vv..Vv..Vvdr.v+.Vvdr.v..Vv.|.v..Vv..Wv..Vvdr.v|.Vvdr.v.. VvRich..Vv.....PE..L.....c.....v.....3.....@.....#..... .....text....J..... ..`.rdata...1.....2.....@..@.data....B...@.....@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.687199505367895
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:	fyTwP4SHWF.exe
File size:	430029
MD5:	d3e933b0aab571bdc73355a106d657e0
SHA1:	ee600eacf16a1075fc8a28116a64f96403122d49
SHA256:	51ab5d042dee8df90162a00a3307cf8d38d12bc54b7dc07c756996aa0f6b3804
SHA512:	db4cf8c673e8fa839ad9af7edd61f00d57d24ba68955e97e4acc2f0a3046c4aa91a63c2a0c3803de3276b6cb7ba1f27f66732e2a023c0d0f484f4b457fc9f42c
SSDEEP:	6144:nYa603Pc/eEb9lh4VB/Q3Eo1z/AMxf09Vi01XpSjROKeOSA3yPKN5nCugfzs0GFD:nYi0GEb9Z87jf+1wdPNiOh7gfzsh1
TLSH:	45940288F8548973EDAA0833FEAAD8055726BD126E650D4972D4BB5B3EB3483C30D753
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:	707070f0c8c8e170

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 00007F96B93C630Ah
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

Instruction
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F96B93C62DAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
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	0x116c8	.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	0x116c8	0x11800	False	0.34814453125	data	5.080230239740608	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b208	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584	English	United States
RT_ICON	0x4ba30	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_DIALOG	0x4be98	0x100	data	English	United States
RT_DIALOG	0x4bf98	0x11c	data	English	United States
RT_DIALOG	0x4c0b8	0x60	data	English	United States
RT_GROUP_ICON	0x4c118	0x22	data	English	United States
RT_VERSION	0x4c140	0x244	data	English	United States
RT_MANIFEST	0x4c388	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

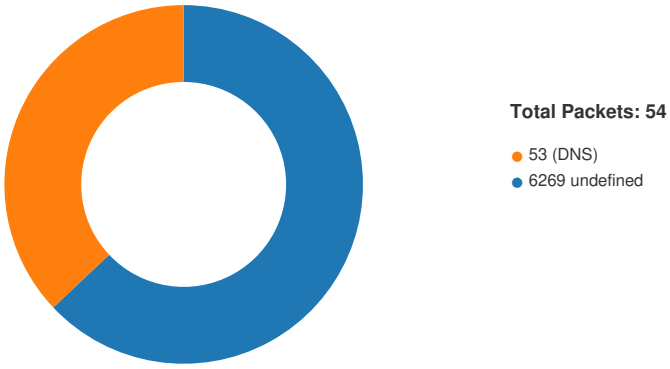
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.745.137.65.132 4973462692816766 02/01/23-05:15:28.676401	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49734	6269	192.168.2.7	45.137.65.132
45.137.65.132192.168.2.7 6269497272841753 02/01/23-05:14:56.574585	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49727	45.137.65.132	192.168.2.7

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
45.137.65.132192.168.2.76269497442841753 02/01/23-05:16:22.394490	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49744	45.137.65.132	192.168.2.7
192.168.2.745.137.65.1324972862692816766 02/01/23-05:15:03.576741	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49728	6269	192.168.2.7	45.137.65.132
192.168.2.745.137.65.1324971162692816766 02/01/23-05:14:19.296579	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49711	6269	192.168.2.7	45.137.65.132
45.137.65.132192.168.2.76269497402810451 02/01/23-05:15:57.113635	TCP	2810451	ETPRO TROJAN NanoCore RAT Keepalive Response 3	6269	49740	45.137.65.132	192.168.2.7
45.137.65.132192.168.2.76269497222841753 02/01/23-05:14:40.350682	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49722	45.137.65.132	192.168.2.7
192.168.2.745.137.65.1324972062692816766 02/01/23-05:14:35.257700	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49720	6269	192.168.2.7	45.137.65.132
45.137.65.132192.168.2.76269497402841753 02/01/23-05:15:57.113635	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49740	45.137.65.132	192.168.2.7
192.168.2.745.137.65.1324973062692816766 02/01/23-05:15:09.580115	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49730	6269	192.168.2.7	45.137.65.132
192.168.2.745.137.65.1324973362692816766 02/01/23-05:15:22.661130	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49733	6269	192.168.2.7	45.137.65.132
45.137.65.132192.168.2.76269497232841753 02/01/23-05:14:46.707897	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49723	45.137.65.132	192.168.2.7
45.137.65.132192.168.2.76269497242841753 02/01/23-05:14:51.698320	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49724	45.137.65.132	192.168.2.7
45.137.65.132192.168.2.76269497412841753 02/01/23-05:16:02.171075	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49741	45.137.65.132	192.168.2.7
45.137.65.132192.168.2.76269497432841753 02/01/23-05:16:07.296877	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49743	45.137.65.132	192.168.2.7
45.137.65.132192.168.2.76269497142810290 02/01/23-05:14:28.429351	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	6269	49714	45.137.65.132	192.168.2.7
192.168.2.745.137.65.1324973762692816766 02/01/23-05:15:41.799633	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49737	6269	192.168.2.7	45.137.65.132
192.168.2.745.137.65.1324974162692816766 02/01/23-05:16:02.177770	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49741	6269	192.168.2.7	45.137.65.132
45.137.65.132192.168.2.76269497392841753 02/01/23-05:15:52.038941	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49739	45.137.65.132	192.168.2.7
192.168.2.745.137.65.1324971462692816766 02/01/23-05:14:29.178500	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49714	6269	192.168.2.7	45.137.65.132
45.137.65.132192.168.2.76269497312841753 02/01/23-05:15:14.788888	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49731	45.137.65.132	192.168.2.7

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
45.137.65.132192.168.2.76269497352841753 02/01/23-05:15:33.801145	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49735	45.137.65.132	192.168.2.7
45.137.65.132192.168.2.76269497382841753 02/01/23-05:15:46.943033	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49738	45.137.65.132	192.168.2.7

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 05:14:18.162858009 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.197880030 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.198355913 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.241461992 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.290383101 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.308535099 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.337692976 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.337827921 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.424077034 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.441468000 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.533484936 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.557157993 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.557209015 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.557250023 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.557296038 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.557595968 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.557595968 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.587589979 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.587625027 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.587646008 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.587665081 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.587683916 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.587702036 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.587721109 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.587738991 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.587958097 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.589979887 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.589979887 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.618155003 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.618196011 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.618218899 CET	6269	49711	45.137.65.132	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 05:14:18.618242979 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.618268013 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.618294001 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.618407965 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.618407965 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.620224953 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.620249987 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.620271921 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.620296001 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.620321035 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.620347977 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.620368958 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.620388985 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.620407104 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.620407104 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.620407104 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.620410919 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.620431900 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.620454073 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.622014046 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.648909092 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.649013042 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.649080992 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.649143934 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.649147987 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.649211884 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.649250031 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.649276972 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.649341106 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.649396896 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.649444103 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.649473906 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.649473906 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.649490118 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.649563074 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.649611950 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.649637938 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.649688005 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.651628971 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.651679039 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.651721001 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.651767015 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.651774883 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.651812077 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.651858091 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.651902914 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.651931047 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.651932001 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.651951075 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.651994944 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.652039051 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.652041912 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.652084112 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.652127981 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.652173042 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.652206898 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.652208090 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.652218103 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.652262926 CET	6269	49711	45.137.65.132	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 05:14:18.652309895 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.652367115 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.653111935 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.654814959 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.654860020 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.654898882 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.654942989 CET	6269	49711	45.137.65.132	192.168.2.7
Feb 1, 2023 05:14:18.655051947 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.655051947 CET	49711	6269	192.168.2.7	45.137.65.132
Feb 1, 2023 05:14:18.679819107 CET	6269	49711	45.137.65.132	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 05:14:18.041230917 CET	60326	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:14:18.148085117 CET	53	60326	8.8.8.8	192.168.2.7
Feb 1, 2023 05:14:24.836009026 CET	50505	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:14:24.942651033 CET	53	50505	8.8.8.8	192.168.2.7
Feb 1, 2023 05:14:34.243309021 CET	63926	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:14:34.261714935 CET	53	63926	8.8.8.8	192.168.2.7
Feb 1, 2023 05:14:40.269475937 CET	51007	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:14:40.287024021 CET	53	51007	8.8.8.8	192.168.2.7
Feb 1, 2023 05:14:46.528229952 CET	50513	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:14:46.639312983 CET	53	50513	8.8.8.8	192.168.2.7
Feb 1, 2023 05:14:51.513125896 CET	60765	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:14:51.619739056 CET	53	60765	8.8.8.8	192.168.2.7
Feb 1, 2023 05:14:56.473234892 CET	49516	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:14:56.494921923 CET	53	49516	8.8.8.8	192.168.2.7
Feb 1, 2023 05:15:01.467236996 CET	62679	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:15:01.485101938 CET	53	62679	8.8.8.8	192.168.2.7
Feb 1, 2023 05:15:08.577121973 CET	52104	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:15:08.594609022 CET	53	52104	8.8.8.8	192.168.2.7
Feb 1, 2023 05:15:14.614614964 CET	65356	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:15:14.723148108 CET	53	65356	8.8.8.8	192.168.2.7
Feb 1, 2023 05:15:19.982728004 CET	51526	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:15:20.000329971 CET	53	51526	8.8.8.8	192.168.2.7
Feb 1, 2023 05:15:27.687212944 CET	51139	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:15:27.795356035 CET	53	51139	8.8.8.8	192.168.2.7
Feb 1, 2023 05:15:33.710380077 CET	58784	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:15:33.729927063 CET	53	58784	8.8.8.8	192.168.2.7
Feb 1, 2023 05:15:38.864883900 CET	64608	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:15:38.973797083 CET	53	64608	8.8.8.8	192.168.2.7
Feb 1, 2023 05:15:46.845508099 CET	58746	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:15:46.863115072 CET	53	58746	8.8.8.8	192.168.2.7
Feb 1, 2023 05:15:51.864135027 CET	62433	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:15:51.969964027 CET	53	62433	8.8.8.8	192.168.2.7
Feb 1, 2023 05:15:56.930159092 CET	61248	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:15:57.037552118 CET	53	61248	8.8.8.8	192.168.2.7
Feb 1, 2023 05:16:02.088044882 CET	52750	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:16:02.105552912 CET	53	52750	8.8.8.8	192.168.2.7
Feb 1, 2023 05:16:07.212547064 CET	50231	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:16:07.229955912 CET	53	50231	8.8.8.8	192.168.2.7
Feb 1, 2023 05:16:12.287746906 CET	58514	53	192.168.2.7	8.8.8.8
Feb 1, 2023 05:16:12.305541992 CET	53	58514	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 1, 2023 05:14:18.041230917 CET	192.168.2.7	8.8.8.8	0xfcd	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:14:24.836009026 CET	192.168.2.7	8.8.8.8	0xbdf7	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:14:34.243309021 CET	192.168.2.7	8.8.8.8	0xded4	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:14:40.269475937 CET	192.168.2.7	8.8.8.8	0x5981	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:14:46.528229952 CET	192.168.2.7	8.8.8.8	0x7e10	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:14:51.513125896 CET	192.168.2.7	8.8.8.8	0xe48f	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:14:56.473234892 CET	192.168.2.7	8.8.8.8	0xcf85	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:01.467236996 CET	192.168.2.7	8.8.8.8	0x2e4b	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:08.577121973 CET	192.168.2.7	8.8.8.8	0xf2bb	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:14.614614964 CET	192.168.2.7	8.8.8.8	0xd1c5	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:19.982728004 CET	192.168.2.7	8.8.8.8	0xd2a7	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:27.687212944 CET	192.168.2.7	8.8.8.8	0xb850	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:33.710380077 CET	192.168.2.7	8.8.8.8	0xff55	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:38.864883900 CET	192.168.2.7	8.8.8.8	0x4880	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:46.845508099 CET	192.168.2.7	8.8.8.8	0xc045	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:51.864135027 CET	192.168.2.7	8.8.8.8	0x6400	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:56.930159092 CET	192.168.2.7	8.8.8.8	0x9958	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:16:02.088044882 CET	192.168.2.7	8.8.8.8	0x39d0	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:16:07.212547064 CET	192.168.2.7	8.8.8.8	0xb515	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:16:12.287746906 CET	192.168.2.7	8.8.8.8	0x7d2e	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false

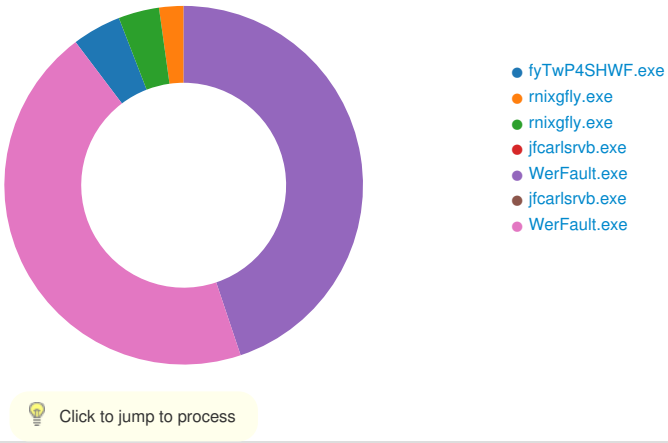
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 05:14:18.148085117 CET	8.8.8.8	192.168.2.7	0xfcd	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:14:24.942651033 CET	8.8.8.8	192.168.2.7	0xbdf7	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:14:34.261714935 CET	8.8.8.8	192.168.2.7	0xded4	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:14:40.287024021 CET	8.8.8.8	192.168.2.7	0x5981	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:14:46.639312983 CET	8.8.8.8	192.168.2.7	0x7e10	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:14:51.619739056 CET	8.8.8.8	192.168.2.7	0xe48f	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:14:56.494921923 CET	8.8.8.8	192.168.2.7	0xcf85	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:01.485101938 CET	8.8.8.8	192.168.2.7	0x2e4b	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:08.594609022 CET	8.8.8.8	192.168.2.7	0xf2bb	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 05:15:14.723148108 CET	8.8.8.8	192.168.2.7	0xd1c5	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:20.000329971 CET	8.8.8.8	192.168.2.7	0xd2a7	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:27.795356035 CET	8.8.8.8	192.168.2.7	0xb850	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:33.729927063 CET	8.8.8.8	192.168.2.7	0xff55	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:38.973797083 CET	8.8.8.8	192.168.2.7	0x4880	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:46.863115072 CET	8.8.8.8	192.168.2.7	0xc045	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:51.969964027 CET	8.8.8.8	192.168.2.7	0x6400	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:15:57.037552118 CET	8.8.8.8	192.168.2.7	0x9958	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:16:02.105552912 CET	8.8.8.8	192.168.2.7	0x39d0	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:16:07.229955912 CET	8.8.8.8	192.168.2.7	0xb515	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 05:16:12.305541992 CET	8.8.8.8	192.168.2.7	0x7d2e	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: fyTwP4SHWF.exe PID: **6032**, Parent PID: **3320**

General

Target ID:	0
Start time:	05:14:08

Start date:	01/02/2023
Path:	C:\Users\user\Desktop\fyTwP4SHWF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\fyTwP4SHWF.exe
Imagebase:	0x400000
File size:	430029 bytes
MD5 hash:	D3E933B0AAB571BDC73355A106D657E0
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~1\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~1\AppData\Local\Temp\nsvBAAB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user~1\AppData\Local\Temp\nsvBAAC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user~1\AppData\Local\Temp\nsvBAAD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
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~1	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~1\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~1\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~1\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~1\AppData\Local\Temp\nsvBAAD.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1	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~1\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~1\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~1\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~1\AppData\Local\Temp\vvnwaf.f	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user~1\AppData\Local\Temp\somvwkehjlp.rt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user~1\AppData\Local\Temp\rnixgfly.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\nsvBAAB.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsvBAAD.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\nsvBAAC.tmp	0	28785	26 36 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 03 00 00 00 fd 19 00 00 79 00 00 00 30 27 00 00 00 00 00 00 40 35 00 00 01 00 00 00 0e 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 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 1c 00 00 00 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 00 00 00 00	&6,y0'@56	success or wait	21	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vvnwaf.f	0	16384	43 73 fd fd 03 77 fd 57 37 fd 33 fd 3d 51 fd 09 08 fd 81 34 fd fd fd 4c 22 fd 4f fd 10 24 4a 7b fd fd 7b fd fd 11 7a fd fd fd fd fd 23 fd 03 2b fd 45 fd fd 34 0b fd 1c 59 fd fd fd 36 fd 29 1c 50 1f 38 6a 0a fd 5e fd 1b fd fd fd 59 fd fd 4d fd 13 6d fd 76 0d 34 41 49 fd 01 2a fd 70 fd 38 fd fd 69 fd 4d 35 fd 5a 2d 75 0e fd 71 fd fd 22 a6 47 e2 3e 19 fd 77 71 18 1a 07 44 fd fd fd 76 03 21 57 fd 62 58 36 fd 2b fd fd 66 fd fd fd fd fd fd fd 3e 23 75 52 53 3e fd 7e 33 fd 24 4f 74 79 fd 7d fd 57 65 4c 14 5d fd 74 fd fd 6f f2 fd fd 59 fd 46 fd 53 fd 46 fd 03 47 fd fd 6b fd fd fd 67 16 fd fd fd 22 1c fd fd 53 2e 11 53 fd fd fd fd 24 fd 1b 01 fd 18 04 fd fd fd 34 68 fd fd fd fd fd 68 28 fd 22 fd fd fd 27 fd	CswW73=Q4L"O$J{{#+E 4Y6)P8^YMmv 4AI*p8iM5Z- uq"G>wqDv!WbX+f>#uR S>~3$Oty}WeL]toYFSFG kg"S.S$4hh"'	success or wait	19	406224	WriteFile
C:\Users\user\AppData\Local\Temp\somvwkehjlp.rt	0	7840	e3 37 30 35 6d fd fd 66 fd 46 3c fd 12 1b 30 35 6f fd 3a fd 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 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 $A5=<r	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\rnixgfly.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4f 65 38 25 0b 04 56 76 0b 04 56 76 0b 04 56 76 64 72 fd 76 2b 04 56 76 64 72 fd 76 18 04 56 76 02 7c fd 76 1e 04 56 76 0b 04 57 76 fd 04 56 76 64 72 fd 76 7c 04 56 76 64 72 fd 76 0a 04 56 76 52 69 63 68 0b 04 56 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd 63 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 0a 00 00 fd 00	MZ@!L!This program cannot be run in DOS mode.$Oe8%VvVvVvdrv + VvdrvVv|vVvWvVvdrv|Vv drvVvRichVvPELc	success or wait	5	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\fyTwP4SHWF.exe	unknown	512	success or wait	208	4061F5	ReadFile
C:\Users\user\Desktop\fyTwP4SHWF.exe	unknown	16384	success or wait	20	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsvBAAC.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsvBAAC.tmp	unknown	13862	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsvBAAC.tmp	unknown	4	success or wait	3	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsvBAAC.tmp	unknown	16384	success or wait	25	4061F5	ReadFile

Analysis Process: rnixgfly.exe PID: **4904**, Parent PID: **6032**

General

Target ID:	1
Start time:	05:14:09
Start date:	01/02/2023
Path:	C:\Users\user\AppData\Local\Temp\rnixgfly.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user~1\AppData\Local\Temp\rnixgfly.exe" C:\Users\user~1\AppData\Local\Temp\somvwkehjlp.rt
Imagebase:	0x400000
File size:	76800 bytes
MD5 hash:	C1DC97853E14C21B463C6E95B21C300C
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: 00000001.00000002.249320721.0000000002210000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.249320721.0000000002210000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.249320721.0000000002210000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.249320721.0000000002210000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.249320721.0000000002210000.00000004.00001000.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.249320721.0000000002210000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 10%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ilkqegcy	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	480414	CreateDirectoryW
C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	480357	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe	0	76800	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 4f 65 38 25 0b 04 56 76 0b 04 56 76 0b 04 56 76 64 72 fd 76 2b 04 56 76 64 72 fd 76 18 04 56 76 02 7c fd 76 1e 04 56 76 0b 04 57 76 fd 04 56 76 64 72 fd 76 7c 04 56 76 64 72 fd 76 0a 04 56 76 52 69 63 68 0b 04 56 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd 63 00 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 0a 00 00 fd 00	MZ@!L!This program cannot be run in DOS mode.$Oe8%VvVvVvdrv + VvdrvVv|vVvWvVvdrv|Vv drvVvRichVvPELc	success or wait	1	480366	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\somvwkehjlp.rt	unknown	4096	success or wait	1	40528A	ReadFile
C:\Users\user\AppData\Local\Temp\somvwkehjlp.rt	unknown	4096	success or wait	1	40528A	ReadFile
C:\Users\user\AppData\Local\Temp\rnixgfly.exe	unknown	76800	success or wait	1	480339	ReadFile
C:\Users\user\AppData\Local\Temp\vvnwaf.f	unknown	287232	success or wait	1	48124E	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	4816C1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	4816C1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	4816C1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	4816C1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	4816C1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	4816C1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	4816C1	ReadFile

Registry Activities

Analysis Process: rnixgfly.exe PID: **3192**, Parent PID: **4904**

General

Target ID:	2
Start time:	05:14:10
Start date:	01/02/2023
Path:	C:\Users\user\AppData\Local\Temp\rnixgfly.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\rnixgfly.exe
Imagebase:	0x400000
File size:	76800 bytes
MD5 hash:	C1DC97853E14C21B463C6E95B21C300C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.508686978.00000000067C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.508686978.00000000067C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.508686978.00000000067C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen

- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.508686978.00000000067C0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.509009346.0000000006860000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.509009346.0000000006860000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.509009346.0000000006860000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.509009346.0000000006860000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.508822078.0000000006800000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.508822078.0000000006800000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.508822078.0000000006800000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.508822078.0000000006800000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.503941570.00000000035E1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.503941570.00000000035E1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.508900878.0000000006830000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.508900878.0000000006830000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.508900878.0000000006830000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.508900878.0000000006830000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.506631236.0000000004F62000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.506631236.0000000004F62000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.506631236.0000000004F62000.00000040.00001000.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.506631236.0000000004F62000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.501682752.00000000005C8000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.501682752.00000000005C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.501682752.00000000005C8000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.501682752.00000000005C8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.507046182.0000000005810000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.507046182.0000000005810000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.507046182.0000000005810000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.507046182.0000000005810000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.508294915.0000000005D60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.508294915.0000000005D60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.508294915.0000000005D60000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.508294915.0000000005D60000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.508782806.00000000067F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.508782806.00000000067F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.508782806.00000000067F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.508782806.00000000067F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.508849965.0000000006810000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.508849965.0000000006810000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.508849965.0000000006810000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.508849965.0000000006810000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.501206954.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.501206954.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.501206954.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.501206954.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.501206954.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.501206954.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.508596907.0000000006640000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.508596907.0000000006640000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.508596907.0000000006640000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.508596907.0000000006640000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.509045139.0000000006870000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.509045139.0000000006870000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.509045139.0000000006870000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.509045139.0000000006870000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.508870070.0000000006820000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.508870070.0000000006820000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.508870070.0000000006820000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.508870070.0000000006820000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.503941570.0000000003575000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.509221233.00000000068B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.509221233.00000000068B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.509221233.00000000068B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.509221233.00000000068B0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.507263839.00000000058C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.507263839.00000000058C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.507263839.00000000058C0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.507263839.00000000058C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.507263839.00000000058C0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.508927189.0000000006840000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.508927189.0000000006840000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.508927189.0000000006840000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.508927189.0000000006840000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.502515145.0000000002490000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.502515145.0000000002490000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.502515145.0000000002490000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.502515145.0000000002490000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.502515145.0000000002490000.00000004.08000000.00040000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.502515145.0000000002490000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.503941570.0000000003851000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.503941570.0000000003851000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.502791120.0000000002551000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.502791120.0000000002551000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.503941570.000000000366D000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.503941570.000000000366D000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.502791120.00000000025CF000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.502791120.00000000025CF000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E3CF06	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	72E3CF06	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	71C8BEFF	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	71C81E60	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	71C8BEFF	CreateDirectoryW
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	71C8BEFF	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	18	71C81E60	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	71C81E60	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	71C81E60	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 3d 38 56 04 fd 48	=8VH	success or wait	1	71C81B4F	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	20	71C81B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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"30tRDn_4dEi~|fX_Xfp^>a$e6:7d(aA=)*{B[y%*iQ<xtXHHF7gI*3{nLy;is-(5iJ5b7}fKHV	success or wait	1	71C81B4F	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	71C81B4F	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	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72E15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C81B4F	ReadFile

Analysis Process: jfcarlsrvb.exe PID: **4528**, Parent PID: **3320**

General

Target ID:	3
Start time:	05:14:21
Start date:	01/02/2023
Path:	C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe" "C:\Users\user~1\AppData\Local\Temp\rnixgfly.exe" C:\Users\user~1\
Imagebase:	0x400000
File size:	76800 bytes
MD5 hash:	C1DC97853E14C21B463C6E95B21C300C
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 10%, ReversingLabs
Reputation:	low

Analysis Process: WerFault.exe PID: **4388**, Parent PID: **4528**

General

Target ID:	6
Start time:	05:14:24
Start date:	01/02/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4528 -s 656
Imagebase:	0xe50000
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	6C9A1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A1.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C99497A	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_jfcarlsrvb.exe_f36b28a8e4f7e8b0d66d5d37aab64913222e2789_70c0d770_117b1399	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_jfcarlsrvb.exe_f36b28a8e4f7e8b0d66d5d37aab64913222e2789_70c0d770_117b1399\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C99497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A1.tmp	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A1.tmp.xml	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BE.tmp.csv	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68A.tmp.txt	success or wait	1	6C99497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 65 fd 63 fd 05 12 00 00 00 00 00	MDMP ec	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1c 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 11 00 00 fd 65 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 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTec Pacific Standard TimePacific Daylight Tim e	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	8630	716	01 00 01 00 00 00 00 00 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 01 2b 00 66 00 2b 00 66 00 00 00 00 00 17 04 00 fd 02 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 fd fd 19 00 78 36 40 00 23 00 19 00 06 02 00 00 fd fd 19 00 2b 00 fd 77 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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+f+fx6@#+w	success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	1620	168	fd 11 00 00 00 00 00 00 17 04 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 78 36 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 21 00 00	x6@!	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	11494	20	0e 00 00 00 3c fd fd 77 00 00 00 00 00 01 00 00 fd 2d 00 00	<w-	success or wait	14	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	11722	256	fd 08 00 fd fd 54 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 55 00 00 00 fd fd fd fd 77 fd fd fd 2c 00 fd fd 56 00 00 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 57 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 58 00 00 00 fd fd fd fd 77 fd fd fd 0c 00 fd fd 59 00 00 00 fd fd fd fd 77 fd fd fd 40 00 fd fd 5a 00 18 00 fd fd fd 77 fd fd fd 04 00 fd fd 5b 00 1d 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 5c 00 00 00 fd fd fd fd 77 fd fd fd 10 00 fd fd 5d 00 00 00 fd fd fd fd 77 fd fd fd 08 00 fd fd 5e 00 00 00 fd fd fd fd 77 fd fd fd 10 00 fd fd 5f 00 00 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 60 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 61 00 07 00 fd fd fd fd 77 fd fd fd 08 00 fd fd 62 00 00 00 fd fd fd fd 77 fd fd fd 1c 00 fd fd 63 00 00 00 fd fd fd fd 77 fd	TwUw,VwWwXwYw@Zw[w\w]w^w_w`wawbwcw	success or wait	13	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	27114	2192	fd fd fd 77 fd 1a 6f 77 fd fd fd fd fd fd 19 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 02 00 00 fd 02 00 00 00 00 00 00 24 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 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 fd 23 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wow$#	success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	9346	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 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 04 fd 19 00 fd fd fd 77 23 00 00 00 06 02 00 00 74 fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w#t+	success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	1888	48	fd 11 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 30 24 00 00 00 00 00 fd fd fd 00 00 00 00 00 3c 02 00 00 fd 67 00 00 fd 02 00 00 1a 2a 00 00	0$<g*	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	7354	34	1c 00 00 00 6a 00 66 00 63 00 61 00 72 00 6c 00 73 00 72 00 76 00 62 00 2e 00 65 00 78 00 65 00 00 00	jfcarlsrvb.exe	success or wait	44	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	6596	752	00 00 fd 73 00 00 00 00 00 00 03 00 fd fd 03 00 fd 2a 2c fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 50 fd 02 00 00 00 00 00 fd 14 03 00 00 00 00 07 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 7d 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 16 31 1b 00 00 00 00 00 2a fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 70 28 06 00 00 00 00	s*,!BB?%@AZbP}1*@p(	success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	29306	9324	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31E.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 2c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 28 1a 00 00 fd 7c 00 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8T(|0	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 34 00 35 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4528</Pid>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6a 00 66 00 63 00 61 00 72 00 6c 00 73 00 72 00 76 00 62 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>jfcarlsrvb.exe</ImageName>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1084	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1182	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 30 00 34 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7042</Uptime>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1232	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1322	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1382	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1436	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 33 00 38 00 39 00 32 00 36 00 30 00 38 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>93892608</PeakVirtualSize>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1532	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 32 00 32 00 35 00 38 00 33 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>92258304</VirtualSize>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 30 00 36 00 33 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>2063</PageFaultCount>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 36 00 36 00 37 00 32 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>7966720</PeakWorkingSetSize>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 36 00 36 00 37 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7966720</WorkingSetSize>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 37 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>177776</QuotaPeakPagedPoolUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 36 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>176984</QuotaPagedPoolUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 37 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>22752</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 34 00 38 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>22480</QuotaNonPagedPoolUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 39 00 34 00 30 00 34 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>1794048</PagefileUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 32 00 32 00 34 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>18022240</PeakPagefileUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 39 00 34 00 30 00 34 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>1794048</PrivateUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3320</Pid>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2832	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2902	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2906	2	09 00		success or wait	4	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	2914	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3004	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3008	2	09 00		success or wait	4	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3016	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 32 00 32 00 35 00 33 00 39 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6225399</Uptime>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3064	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3068	2	09 00		success or wait	4	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3076	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3166	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3230	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3288	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3378	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3382	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3392	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3466	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3470	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3480	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 35 00 37 00 31 00 39 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>57199</PageFaultCount>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3556	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3560	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3570	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 33 00 34 00 34 00 31 00 31 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>123441152</PeakWorkingSetSize>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3670	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3674	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3684	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 33 00 30 00 30 00 32 00 38 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>123002880</WorkingSetSize>	success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3768	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3772	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3782	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 32 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11421 60</QuotaPeakPagedPoolUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3898	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3902	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	3912	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 34 00 35 00 36 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 >1084560</ QuotaPagedPoolUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4012	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4016	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4026	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 39 00 32 00 34 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>92 496</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4150	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4154	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4164	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 30 00 33 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>80344< /QuotaNonPagedPoolUsage>	success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4272	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4276	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4286	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 35 00 37 00 31 00 39 00 35 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4571955 2</PagefileUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4364	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4368	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4378	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 37 00 30 00 37 00 31 00 32 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>47 071232</P eakPagefileUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4472	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4476	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4486	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 35 00 37 00 31 00 39 00 35 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4571955 2</PrivateUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4560	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4564	2	09 00		success or wait	4	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4572	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4618	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4622	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4628	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4670	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4674	2	09 00		success or wait	2	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4678	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4716	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4764	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4802	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4806	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4810	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4862	4	0d 00 0a 00		success or wait	9	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4866	2	09 00		success or wait	18	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	4870	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6a 00 66 00 63 00 61 00 72 00 6c 00 73 00 72 00 76 00 62 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>jfcarlsrvb.exe</Parameter0>	success or wait	9	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	5548	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	5552	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	5554	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	5594	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	5598	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	5600	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	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	5638	4	0d 00 0a 00		success or wait	6	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	5642	2	09 00		success or wait	12	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	5646	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6200	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6204	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6206	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6246	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6250	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6252	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6290	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6294	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6298	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6392	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6396	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6400	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 6f 00 78 00 62 00 74 00 79 00 72 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>oxbtyr, Inc.</SystemManufacturer>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6506	4	0d 00 0a 00		success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6510	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6514	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 6f 00 78 00 62 00 74 00 79 00 72 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>oxbtyr7,1</SystemProductName>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6610	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6614	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6618	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6738	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6742	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6746	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 35 00 30 00 34 00 39 00 32 00 33 00 30 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>1615049230</OSInstallDate>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6828	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6832	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6836	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6938	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6942	2	09 00		success or wait	2	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	6946	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7014	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7018	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7020	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7060	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7064	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7066	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7108	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7204	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7208	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7210	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7246	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7250	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7252	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7276	4	0d 00 0a 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7280	2	09 00		success or wait	6	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7284	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7530	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7534	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7536	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7568	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 31 00 54 00 31 00 33 00 3a 00 31 00 34 00 3a 00 32 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-02-01T13:14:28Z">	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7668	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7672	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7676	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 32 00 39 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 35 00 32 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 31 00 31 00 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 31 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="296" PID="4528" UptimeMS="1171" TimeSinceCreationMS="1171" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7946	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	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7966	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7970	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	7972	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	8010	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	8014	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	8016	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	8054	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	8058	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	8062	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 33 00 66 00 39 00 32 00 64 00 61 00 33 00 2d 00 62 00 35 00 62 00 35 00 2d 00 34 00 63 00 64 00 38 00 2d 00 61 00 36 00 37 00 64 00 2d 00 31 00 39 00 39 00 36 00 34 00 65 00 65 00 66 00 34 00 62 00 63 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>63f92da3-b5b5-4cd8-a67d-19964eef4bcf</Guid>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	8160	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	8164	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	8168	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 31 00 54 00 31 00 33 00 3a 00 31 00 34 00 3a 00 32 00 38 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>2023-02-01T13:14:28Z</CreationTime>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	8266	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	8270	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	8272	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	8312	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER571.tmp.WERInternalMetadata.xml	8316	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	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A1.tmp.xml	0	4664	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_jfcarlsrvb.exe_f36b28a8e4f7e8b0d66d5d37aab64913222e2789_70c0d770_117b1399\Report.wer	0	2	fd fd		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_jfcarlsrvb.exe_f36b28a8e4f7e8b0d66d5d37aab64913222e2789_70c0d770_117b1399\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	171	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_jfcarlsrvb.exe_f36b28a8e4f7e8b0d66d5d37aab64913222e2789_70c0d770_117b1399\Report.wer	11640	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 33 00 36 00 38 00 39 00 36 00 30 00 31 00 32 00 31 00	MetadataHash=1368960121	success or wait	1	6C99497A	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: jfcarlsrvb.exe PID: **5880**, Parent PID: **3320**

General

Target ID:	7
Start time:	05:14:30
Start date:	01/02/2023
Path:	C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe" "C:\Users\user~1\AppData\Local\Temp\rnixgfly.exe" C:\Users\user~1\
Imagebase:	0x400000
File size:	76800 bytes
MD5 hash:	C1DC97853E14C21B463C6E95B21C300C
Has elevated privileges:	false

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

Analysis Process: WerFault.exe PID: **5912**, Parent PID: **5880**

General

Target ID:	9
Start time:	05:14:31
Start date:	01/02/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5880 -s 628
Imagebase:	0xe50000
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	6C9A1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17A2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17A2.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C99497A	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_jfcarlsrvb.exe_f36b28a8e4f7e8b0d66d5d37aab64913222e2789_70c0d770_17471e38	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_jfcarlsrvb.exe_f36b28a8e4f7e8b0d66d5d37aab64913222e2789_70c0d770_17471e38\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C99497A	unknown

File Deleted				
File Path	**Completion**	**Count**	**Source Address**	**Symbol**
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17A2.tmp	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17A2.tmp.xml	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17C2.tmp.csv	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19B7.tmp.txt	success or wait	1	6C99497A	unknown

File Written								
File Path	**Offset**	**Length**	**Value**	**Ascii**	**Completion**	**Count**	**Source Address**	**Symbol**
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 65 fd 63 fd 05 12 00 00 00 00 00	MDMP ec	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	7240	6	00 00 00 00 00 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.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 48 1c 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 16 00 00 fd 65 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 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBHGenuineIntelWTec Pacific Standard TimePacific Daylight Ti me	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	8494	716	01 00 01 00 00 00 00 00 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 fd 2b 00 00 00 53 00 00 01 2b 00 68 00 2b 00 00 00 00 00 00 00 17 04 00 fd 02 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 fd fd 19 00 78 36 40 00 23 00 19 00 06 02 00 00 fd fd 19 00 2b 00 fd 77 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S+h+x6@#+w	success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	1620	168	fd 16 00 00 00 00 00 00 17 04 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 78 36 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 2e 21 00 00	x6@.!	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	11358	20	0e 00 00 00 3c fd fd 77 00 00 00 00 00 01 00 00 42 2d 00 00	<wB-	success or wait	14	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	11586	256	fd 08 00 fd fd 54 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 55 00 00 00 fd fd fd fd 77 fd fd fd 2c 00 fd fd 56 00 00 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 57 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 58 00 00 00 fd fd fd fd 77 fd fd fd 0c 00 fd fd 59 00 00 00 fd fd fd fd 77 fd fd fd 40 00 fd fd 5a 00 18 00 fd fd fd 77 fd fd fd 04 00 fd fd 5b 00 1d 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 5c 00 00 00 fd fd fd fd 77 fd fd fd 10 00 fd fd 5d 00 00 00 fd fd fd fd 77 fd fd fd 08 00 fd fd 5e 00 00 00 fd fd fd fd 77 fd fd fd 10 00 fd fd 5f 00 00 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 60 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 61 00 07 00 fd fd fd fd 77 fd fd fd 08 00 fd fd 62 00 00 00 fd fd fd fd 77 fd fd fd 1c 00 fd fd 63 00 00 00 fd fd fd fd 77 fd	TwUw,VwWwXwYw@Zw[w\w]w^w_w`wawbwcw	success or wait	13	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	26978	2192	fd fd fd 77 fd 1a 6f 77 fd fd fd fd fd fd 19 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 70 02 00 00 6c 02 00 00 00 00 00 00 24 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 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 fd 2a 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wowpl$*	success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	9210	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 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 04 fd 19 00 fd fd fd 77 23 00 00 00 06 02 00 00 74 fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w#t+	success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	1888	48	fd 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 70 2b 00 00 00 00 00 fd fd fd 00 00 00 00 00 3c 02 00 00 42 30 00 00 fd 02 00 00 fd 29 00 00	p+<B0)	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	1948	4	2b 00 00 00	+	success or wait	43	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	7246	34	1c 00 00 00 6a 00 66 00 63 00 61 00 72 00 6c 00 73 00 72 00 76 00 62 00 2e 00 65 00 78 00 65 00 00 00	jfcarlsrvb.exe	success or wait	43	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	6488	752	00 00 fd 73 00 00 00 00 00 00 03 00 fd fd 03 00 fd 2a 2c fd 10 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 3e 02 00 00 00 00 00 fd 14 03 00 00 00 00 75 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 7f 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 27 1b 00 00 00 00 00 78 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 70 28 06 00 00 00 00	s*,!BB?%@AZbu'x@p(	success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	29170	9044	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14E1.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 28 12 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 5e 2c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 10 19 00 00 36 7c 00 00 15 00 00 00 fd 01 00 00 fd 19 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	(^,T8T6|	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 38 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5880</Pid>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6a 00 66 00 63 00 61 00 72 00 6c 00 73 00 72 00 76 00 62 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>jfcarlsrvb.exe</ImageName>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1084	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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>000 00002</Cm dLineSignature>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1182	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 33 00 34 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2345</Uptime>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1232	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1322	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1382	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1436	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 32 00 30 00 30 00 34 00 33 00 35 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>92004352</PeakVirtualSize>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1532	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 31 00 36 00 31 00 35 00 32 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>91615232</VirtualSize>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 39 00 36 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1961</PageFaultCount>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 36 00 33 00 39 00 30 00 34 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>7639040</PeakWorkingSetSize>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 36 00 33 00 39 00 30 00 34 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>7639040</WorkingSetSize>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 36 00 35 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>176520</QuotaPeakPagedPoolUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 35 00 37 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>175728</QuotaPagedPoolUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 32 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>22264</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 39 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21992</QuotaNonPagedPoolUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 34 00 34 00 38 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1744896</PagefileUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 35 00 33 00 30 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1753088</PeakPagefileUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 34 00 34 00 38 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1744896</PrivateUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3320</Pid>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2832	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2902	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2906	2	09 00		success or wait	4	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	2914	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3004	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3008	2	09 00		success or wait	4	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3016	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 32 00 32 00 39 00 39 00 34 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6229940</Uptime>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3064	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3068	2	09 00		success or wait	4	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3076	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3166	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3230	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3288	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3378	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3382	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3392	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3466	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3470	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3480	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 35 00 37 00 32 00 38 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>57285</PageFaultCount>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3556	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3560	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3570	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 33 00 34 00 34 00 31 00 31 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>123441152</PeakWorkingSetSize>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3670	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3674	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3684	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 31 00 39 00 30 00 35 00 31 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>121905152</WorkingSetSize>	success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3768	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3772	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3782	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 32 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11421 60</QuotaPeakPagedPoolUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3898	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3902	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	3912	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 37 00 32 00 32 00 38 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 >1072280</ QuotaPagedPoolUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4012	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4016	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4026	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 39 00 32 00 34 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>92 496</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4150	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4154	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4164	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 37 00 38 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>78440< /QuotaNonPagedPoolUsage>	success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4272	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4276	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4286	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 35 00 34 00 31 00 36 00 34 00 34 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>45416448</PagefileUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4364	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4368	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4378	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 37 00 30 00 37 00 31 00 32 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>47071232</PeakPagefileUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4472	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4476	2	09 00		success or wait	5	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4486	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 35 00 34 00 31 00 36 00 34 00 34 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>45416448</PrivateUsage>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4560	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4564	2	09 00		success or wait	4	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4572	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4618	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4622	2	09 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4628	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4670	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4674	2	09 00		success or wait	2	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4678	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4716	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4764	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4802	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4806	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4810	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4862	4	0d 00 0a 00		success or wait	9	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4866	2	09 00		success or wait	18	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	4870	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6a 00 66 00 63 00 61 00 72 00 6c 00 73 00 72 00 76 00 62 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>jfcarlsrvb.exe</Parameter0>	success or wait	9	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	5548	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	5552	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	5554	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	5594	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	5598	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	5600	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	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	5638	4	0d 00 0a 00		success or wait	6	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	5642	2	09 00		success or wait	12	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	5646	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6200	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6204	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6206	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6246	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6250	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6252	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6290	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6294	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6298	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6392	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6396	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6400	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 6f 00 78 00 62 00 74 00 79 00 72 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>oxbtyr, Inc.</SystemManufacturer>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6506	4	0d 00 0a 00		success or wait	1	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6510	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6514	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 6f 00 78 00 62 00 74 00 79 00 72 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>oxbtyr7,1</SystemProductName>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6610	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6614	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6618	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6738	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6742	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6746	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 35 00 30 00 34 00 39 00 32 00 33 00 30 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>1615049230</OSInstallDate>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6828	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6832	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6836	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6938	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6942	2	09 00		success or wait	2	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	6946	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7014	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7018	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7020	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7060	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7064	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7066	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7108	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7204	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7208	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7210	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7246	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7250	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7252	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7276	4	0d 00 0a 00		success or wait	3	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7280	2	09 00		success or wait	6	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7284	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7528	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7532	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7534	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7560	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7564	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7566	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 31 00 54 00 31 00 33 00 3a 00 31 00 34 00 3a 00 33 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-02-01T13:14:32Z">	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7666	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7670	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7674	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 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 38 00 38 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 38 00 35 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 38 00 35 00 39 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="301" PID="5880" UptimeMS="859" TimeSinceCreationMS="859" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7932	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7936	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7940	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	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7960	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7964	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	7966	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	8004	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	8008	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	8010	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	8056	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 66 00 34 00 39 00 32 00 62 00 64 00 35 00 2d 00 31 00 32 00 33 00 32 00 2d 00 34 00 30 00 61 00 30 00 2d 00 61 00 39 00 35 00 33 00 2d 00 65 00 65 00 63 00 32 00 63 00 34 00 63 00 66 00 33 00 66 00 31 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>cf492bd5-1232-40a0-a953-eec2c4cf3f11</Guid>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	8154	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	8158	2	09 00		success or wait	2	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	8162	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 31 00 54 00 31 00 33 00 3a 00 31 00 34 00 3a 00 33 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-02-01T13:14:32Z</CreationTime>	success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	8260	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	8264	2	09 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	8266	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	8306	4	0d 00 0a 00		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1705.tmp.WERInternalMetadata.xml	8310	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	6C99497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17A2.tmp.xml	0	4664	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	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_jfcarlsrvb.exe_f36b28a8e4f7e8b0d66d5d37aab64913222e2789_70c0d770_17471e38\Report.wer	0	2	fd fd		success or wait	1	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_jfcarlsrvb.exe_f36b28a8e4f7e8b0d66d5d37aab64913222e2789_70c0d770_17471e38\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	170	6C99497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_jfcarlsrvb.exe_f36b28a8e4f7e8b0d66d5d37aab64913222e2789_70c0d770_17471e38\Report.wer	11540	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 37 00 38 00 35 00 34 00 34 00 38 00 32 00 37 00 33 00	MetadataHash=785448273	success or wait	1	6C99497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly