ID: 799403
Sample Name: lb64ly4W4e.exe
Cookbook: default.jbs
Time: 14:11:08
Date: 06/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

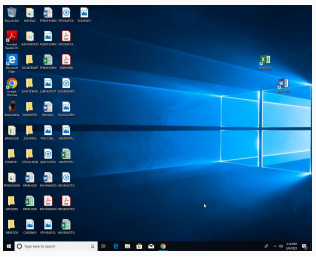
Windows Analysis Report

lb64ly4W4e.exe

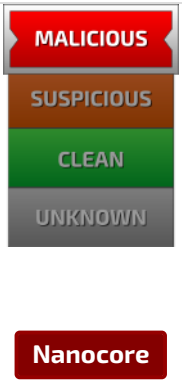
Overview

General Information

Sample Name:	lb64ly4W4e.exe
Analysis ID:	799403
MD5:	4c7df43e37814..
SHA1:	c2315cba4dc1…
SHA256:	49cc6f25d16cf…
Tags:	exe NanoCore RAT
Infos:	



Detection



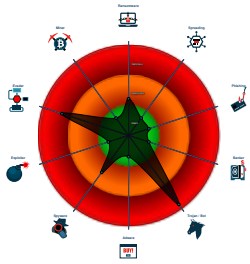
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Maps a DLL or memory area into an…
- Found evasive API chain (may stop…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses dynamic DNS services

Classification



Process Tree

- **System is w10x64**
- lb64ly4W4e.exe (PID: 4332 cmdline: C:\Users\user\Desktop\lb64ly4W4e.exe MD5: 4C7DF43E37814754AD1C8A97AB971AF8)
  - tohjyweui.exe (PID: 5884 cmdline: "C:\Users\user\AppData\Local\Temp\tohjyweui.exe" C:\Users\user\AppData\Local\Temp\fwbfw.c MD5: 64517EEC55E1F3C392B63B73D833E5F9)
    - tohjyweui.exe (PID: 4560 cmdline: C:\Users\user\AppData\Local\Temp\tohjyweui.exe MD5: 64517EEC55E1F3C392B63B73D833E5F9)
  - tpyienirbwgp.exe (PID: 5716 cmdline: "C:\Users\user\AppData\Roaming\swschqavfbk\tpyienirbwgp.exe" "C:\Users\user\AppData\Local\Temp\tohjyweui.exe" C:\Users\user\A MD5: 64517EEC55E1F3C392B63B73D833E5F9)
    - WerFault.exe (PID: 5420 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5716 -s 632 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - tpyienirbwgp.exe (PID: 5408 cmdline: "C:\Users\user\AppData\Roaming\swschqavfbk\tpyienirbwgp.exe" "C:\Users\user\AppData\Local\Temp\tohjyweui.exe" C:\Users\user\A MD5: 64517EEC55E1F3C392B63B73D833E5F9)
    - WerFault.exe (PID: 4032 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5408 -s 604 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "d046c01c-51f5-4c8c-b5b9-b566d533",
  "Group": "",
  "Domain1": "alertt.duckdns.org",
  "Domain2": "alertt.duckdns.org",
  "Port": 6445,
  "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
00000001.00000002.320288694.0000000000630000.00000004.00001000.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x237e5:$x1: NanoCore.ClientPluginHost • 0x23822:$x2: IClientNetworkHost • 0x27355:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.320288694.0000000000630000.00000004.00001000.00020000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x2355d:$x1: NanoCore Client.exe • 0x237e5:$x2: NanoCore.ClientPluginHost • 0x24e1e:$s1: PluginCommand • 0x24e12:$s2: FileCommand • 0x25cc3:$s3: PipeExists • 0x2ba7a:$s4: PipeCreated • 0x2380f:$s5: IClientLoggingHost
00000001.00000002.320288694.0000000000630000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000001.00000002.320288694.0000000000630000.00000004.00001000.00020000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x2354d:$x1: NanoCore Client • 0x2355d:$x1: NanoCore Client • 0x237a5:$x2: NanoCore.ClientPlugin • 0x237e5:$x3: NanoCore.ClientPluginHost • 0x2379a:$i1: IClientApp • 0x237bb:$i2: IClientData • 0x237c7:$i3: IClientNetwork • 0x237d6:$i4: IClientAppHost • 0x237ff:$i5: IClientDataHost • 0x2380f:$i6: IClientLoggingHost • 0x23822:$i7: IClientNetworkHost • 0x23835:$i8: IClientUIHost • 0x23843:$i9: IClientNameObjectCollection • 0x2385f:$i10: IClientReadOnlyNameObjectCollection • 0x235ac:$s1: ClientPlugin • 0x237ae:$s1: ClientPlugin • 0x23ca2:$s2: EndPoint • 0x23cab:$s3: IPAddress • 0x23cb5:$s4: IPEndPoint • 0x256eb:$s6: get_ClientSettings • 0x25c8f:$s7: get_Connected

Source	Rule	Description	Author	Strings
00000001.00000002.320288694.0000000000630000.00000004.00001000.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2354d:$a: NanoCore • 0x2355d:$a: NanoCore • 0x23791:$a: NanoCore • 0x237a5:$a: NanoCore • 0x237e5:$a: NanoCore • 0x235ac:$b: ClientPlugin • 0x237ae:$b: ClientPlugin • 0x237ee:$b: ClientPlugin • 0x236d3:$c: ProjectData • 0x240da:$d: DESCrypto • 0x2baa6:$e: KeepAlive • 0x29a94:$g: LogClientMessage • 0x25c8f:$i: get_Connected • 0x24410:$j: #=q • 0x24440:$j: #=q • 0x2445c:$j: #=q • 0x2448c:$j: #=q • 0x244a8:$j: #=q • 0x244c4:$j: #=q • 0x244f4:$j: #=q • 0x24510:$j: #=q
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.tohjyweui.exe.643658.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
1.2.tohjyweui.exe.643658.1.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$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.tohjyweui.exe.643658.1.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
1.2.tohjyweui.exe.643658.1.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:$s7: get_Connected
1.2.tohjyweui.exe.643658.1.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$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 19 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: 192.168.2.5 - Destination IP: 45.132.106.37

Timestamp:	192.168.2.545.132.106.374971264452816766 02/06/23-14:12:55.395066
SID:	2816766
Source Port:	49712
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5

Timestamp:	45.132.106.37192.168.2.56445497312841753 02/06/23-14:13:52.517965
SID:	2841753
Source Port:	6445
Destination Port:	49731
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37

Timestamp:	192.168.2.545.132.106.374970964452816766 02/06/23-14:12:39.702248
SID:	2816766
Source Port:	49709
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5

Timestamp:	45.132.106.37192.168.2.56445497072841753 02/06/23-14:12:33.506820
SID:	2841753
Source Port:	6445
Destination Port:	49707
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37

Timestamp:	192.168.2.545.132.106.374973564452816766 02/06/23-14:14:08.694757
SID:	2816766

Source Port:	49735
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	−
Timestamp:	45.132.106.37192.168.2.56445497202841753 02/06/23-14:13:12.771040
SID:	2841753
Source Port:	6445
Destination Port:	49720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	−
Timestamp:	192.168.2.545.132.106.374972964452816766 02/06/23-14:13:42.328059
SID:	2816766
Source Port:	49729
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	−
Timestamp:	192.168.2.545.132.106.374970264452816766 02/06/23-14:12:20.468192
SID:	2816766
Source Port:	49702
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	−
Timestamp:	45.132.106.37192.168.2.56445497252841753 02/06/23-14:13:29.137140
SID:	2841753
Source Port:	6445
Destination Port:	49725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Nanocore Checkin Pattern - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	−
Timestamp:	192.168.2.545.132.106.374971164452823337 02/06/23-14:12:50.979729
SID:	2823337
Source Port:	49711
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 3 - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	−
Timestamp:	45.132.106.37192.168.2.56445497202810451 02/06/23-14:13:12.771040
SID:	2810451
Source Port:	6445
Destination Port:	49720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	−
Timestamp:	45.132.106.37192.168.2.56445497332841753 02/06/23-14:13:57.153095
SID:	2841753
Source Port:	6445
Destination Port:	49733
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	
Timestamp:	45.132.106.37192.168.2.56445497352841753 02/06/23-14:14:08.617792
SID:	2841753
Source Port:	6445
Destination Port:	49735
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	
Timestamp:	45.132.106.37192.168.2.56445497362841753 02/06/23-14:14:13.470154
SID:	2841753
Source Port:	6445
Destination Port:	49736
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	
Timestamp:	192.168.2.545.132.106.374972264452816766 02/06/23-14:13:18.836838
SID:	2816766
Source Port:	49722
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	
Timestamp:	192.168.2.545.132.106.374971664452816766 02/06/23-14:12:59.871071
SID:	2816766
Source Port:	49716
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	
Timestamp:	192.168.2.545.132.106.374970364452816766 02/06/23-14:12:29.256960
SID:	2816766
Source Port:	49703
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	
Timestamp:	192.168.2.545.132.106.374972664452816766 02/06/23-14:13:33.513858
SID:	2816766
Source Port:	49726
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	
Timestamp:	45.132.106.37192.168.2.56445497272841753 02/06/23-14:13:37.915437
SID:	2841753
Source Port:	6445
Destination Port:	49727
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	
Timestamp:	45.132.106.37192.168.2.56445497292841753 02/06/23-14:13:42.158315
SID:	2841753
Source Port:	6445

Destination Port:	49729
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	▬
Timestamp:	45.132.106.37192.168.2.56445497022841753 02/06/23-14:12:20.379177
SID:	2841753
Source Port:	6445
Destination Port:	49702
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	▬
Timestamp:	45.132.106.37192.168.2.56445497262841753 02/06/23-14:13:33.469565
SID:	2841753
Source Port:	6445
Destination Port:	49726
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	▬
Timestamp:	192.168.2.545.132.106.374973364452816766 02/06/23-14:13:57.290193
SID:	2816766
Source Port:	49733
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	▬
Timestamp:	45.132.106.37192.168.2.56445497012841753 02/06/23-14:12:15.717836
SID:	2841753
Source Port:	6445
Destination Port:	49701
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	▬
Timestamp:	192.168.2.545.132.106.374970764452816766 02/06/23-14:12:33.686837
SID:	2816766
Source Port:	49707
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	▬
Timestamp:	45.132.106.37192.168.2.56445497122841753 02/06/23-14:12:55.336364
SID:	2841753
Source Port:	6445
Destination Port:	49712
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	▬
Timestamp:	45.132.106.37192.168.2.56445497162841753 02/06/23-14:12:59.766454
SID:	2841753
Source Port:	6445
Destination Port:	49716
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	
Timestamp:	45.132.106.37192.168.2.56445497192841753 02/06/23-14:13:08.445515
SID:	2841753
Source Port:	6445
Destination Port:	49719
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	
Timestamp:	192.168.2.545.132.106.374972364452816766 02/06/23-14:13:24.891407
SID:	2816766
Source Port:	49723
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	
Timestamp:	45.132.106.37192.168.2.56445497172841753 02/06/23-14:13:04.143032
SID:	2841753
Source Port:	6445
Destination Port:	49717
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	
Timestamp:	45.132.106.37192.168.2.56445497112841753 02/06/23-14:12:50.916490
SID:	2841753
Source Port:	6445
Destination Port:	49711
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	
Timestamp:	192.168.2.545.132.106.374971764452816766 02/06/23-14:13:04.199805
SID:	2816766
Source Port:	49717
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	
Timestamp:	192.168.2.545.132.106.374972764452816766 02/06/23-14:13:37.920388
SID:	2816766
Source Port:	49727
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	
Timestamp:	192.168.2.545.132.106.374973064452816766 02/06/23-14:13:48.218570
SID:	2816766
Source Port:	49730
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	
Timestamp:	192.168.2.545.132.106.374972264452816718 02/06/23-14:13:18.233724
SID:	2816718
Source Port:	49722

Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	−
Timestamp:	192.168.2.545.132.106.374973464452816766 02/06/23-14:14:04.014579
SID:	2816766
Source Port:	49734
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	−
Timestamp:	192.168.2.545.132.106.374971064452816766 02/06/23-14:12:46.639827
SID:	2816766
Source Port:	49710
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	−
Timestamp:	192.168.2.545.132.106.374972064452816766 02/06/23-14:13:12.842490
SID:	2816766
Source Port:	49720
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	−
Timestamp:	192.168.2.545.132.106.374971164452816766 02/06/23-14:12:50.979729
SID:	2816766
Source Port:	49711
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	−
Timestamp:	192.168.2.545.132.106.374973164452816766 02/06/23-14:13:52.687469
SID:	2816766
Source Port:	49731
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	−
Timestamp:	192.168.2.545.132.106.374970164452816766 02/06/23-14:12:15.779461
SID:	2816766
Source Port:	49701
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	−
Timestamp:	192.168.2.545.132.106.374972564452816766 02/06/23-14:13:29.249183
SID:	2816766
Source Port:	49725
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 45.132.106.37 - Destination IP: 192.168.2.5	
Timestamp:	45.132.106.37192.168.2.56445497092810290 02/06/23-14:12:38.309927
SID:	2810290
Source Port:	6445
Destination Port:	49709
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	
Timestamp:	192.168.2.545.132.106.374971964452816766 02/06/23-14:13:08.627802
SID:	2816766
Source Port:	49719
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.5 - Destination IP: 45.132.106.37	
Timestamp:	192.168.2.545.132.106.374970364452816718 02/06/23-14:12:27.309652
SID:	2816718
Source Port:	49703
Destination Port:	6445
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for dropped file
- Yara detected Nanocore RAT

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)

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

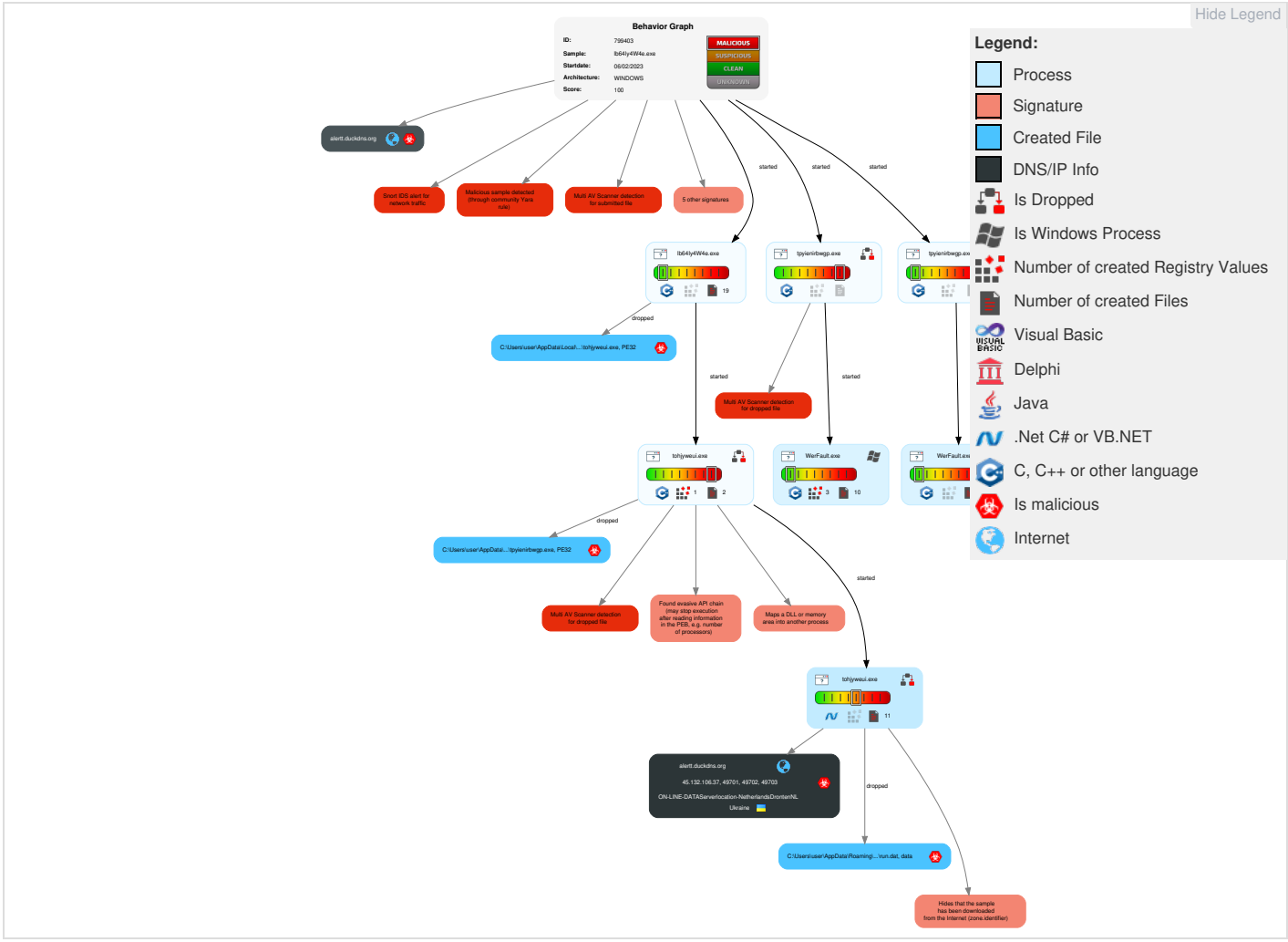
Detected Nanocore Rat

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 1 Windows Service	1 Access Token Manipulation	1 Disable or Modify Tools	1 Input Capture	1 System Time Discovery	Remote Services	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 1 Native API	1 Registry Run Keys / Startup Folder	1 1 Windows Service	1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	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 1 1 Process Injection	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	1 Service Execution	Logon Script (Mac)	1 Registry Run Keys / Startup Folder	1 Masquerading	NTDS	1 3 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	2 1 Virtualization/Sandbox Evasion	LSA Secrets	1 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	1 Access Token Manipulation	Cached Domain Credentials	2 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 1 1 Process Injection	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 Hidden Files and Directories	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

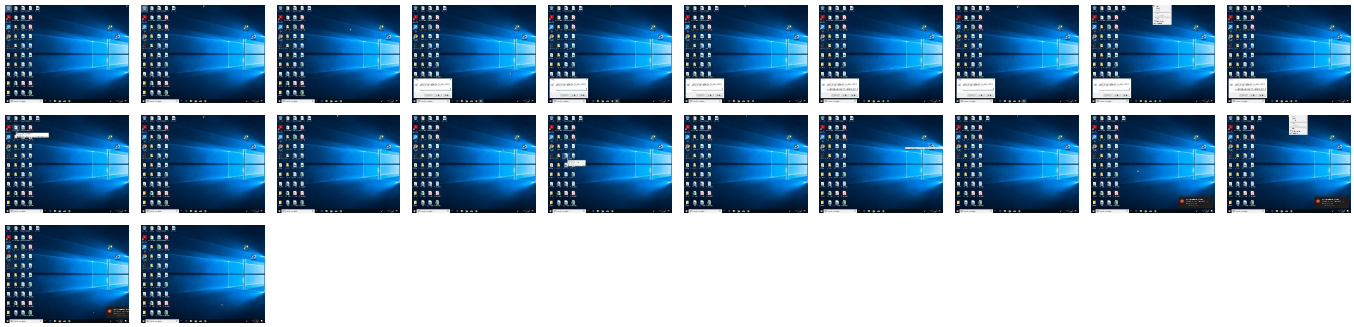
Behavior Graph



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
lb64ly4W4e.exe	41%	ReversingLabs	Win32.Trojan.Nemesis	
lb64ly4W4e.exe	35%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\tohjyweui.exe	23%	ReversingLabs	Win32.Trojan.Pwsx	
C:\Users\user\AppData\Local\Temp\tohjyweui.exe	29%	Virustotal		Browse
C:\Users\user\AppData\Roaming\swschqavfbk\tpyienirbwgp.exe	23%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
alertt.duckdns.org	0%	Avira URL Cloud	safe	
alertt.duckdns.org	1%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
alertt.duckdns.org	45.132.106.37	true	true	• 1%, Virustotal, Browse	unknown

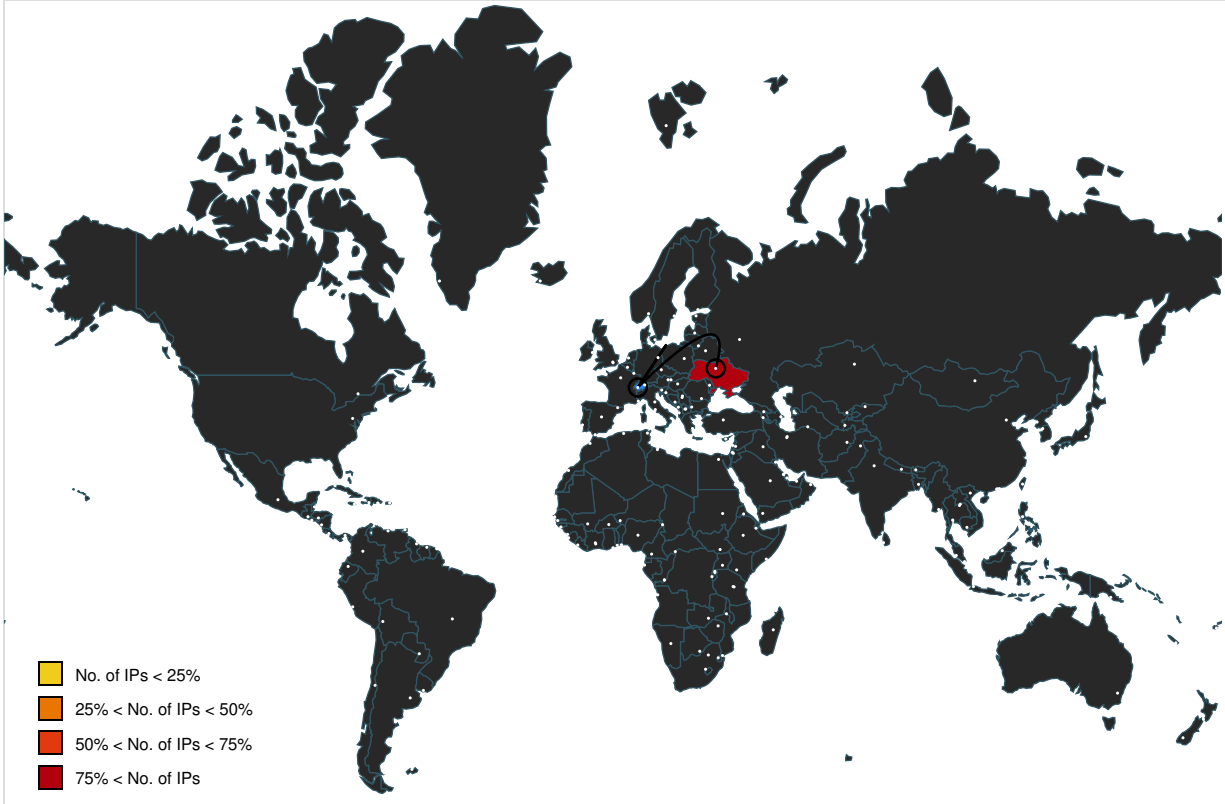
Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	lb64Iy4W4e.exe	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.132.106.37	alertt.duckdns.org	Ukraine		204601	ON-LINE-DATAServerlocation-NetherlandsDrontenNL	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	799403
Start date and time:	2023-02-06 14:11:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 17s
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:	13
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:	lb64Iy4W4e.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/17@24/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.2% (good quality ratio 96.5%) • Quality average: 87.9% • Quality standard deviation: 23.3%
HCA Information:	• Successful, ratio: 90% • 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, WMIADAP.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.168.117.173, 104.208.16.94
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, client.wns.windows.com, blobcollector.events.data.trafficmanager.net, 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.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:12:13	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run luqajfoxt C:\Users\user\AppData\Roaming\swschqavfbk\tpyienirbwgp.exe "C:\Users\user\AppData\Local\Temp\tohjyweui.exe" C:\Users\user\A
14:12:14	API Interceptor	941x Sleep call for process: tohjyweui.exe modified
14:12:21	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run luqajfoxt C:\Users\user\AppData\Roaming\swschqavfbk\tpyienirbwgp.exe "C:\Users\user\AppData\Local\Temp\tohjyweui.exe" C:\Users\user\A
14:12:30	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_tpyienirbwgp.exe_491668454d7886d02c78a9f3324eec6e9b560bc_bb377917_0f868df3\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):	0.929195913406343
Encrypted:	false
SSDEEP:	96:P5F7FbJUSjhRB70sSYpXlQcQmc6ycE8cw3yo++HbHgH3qTP+aVDPMbspoxGfnFhy:hJFbaoHY2GWoPjAQ+t/u7sFS274ltS
MD5:	96F6FB1E217DD003DCE5D7238773460B
SHA1:	89EAE1F997D7756D0AAEC192DE81E69178E6A4AF
SHA-256:	8C67EC275CAAFC86880994975244BCC733DD7348C732D69653E4F0C6E21279DC
SHA-512:	8CE3A7D0FE251B4B304FE130FEDEB9FC8C6D9580F0074C765968A5165D4030B0DE8D52B8A394FFCCC1760162AA4114F07E7CEA6DD3E6FB83F43D0C68BF465E9A
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.=.1.3.3.2.0.1.9.5.1.5.1.3.1.3.7.4.4.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.0.1.9.5.1.5.2.3.1.3.7.4.6.7.....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.b.c.f.c.8.1.3.-.1.b.6.1.-.4.3.f.7.-.9.a.d.6.-.c.0.e.b.a.3.6.2.8.a.6.e.....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.=.6.d.6.a.5.e.9.2.-.5.1.2.b.-.4.9.9.0.-.b.8.7.f.-.4.1.1.f.6.d.f.8.7.b.3.d.....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.=.t.p.y.i.e.n.i.r.b.w.g.p...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.2.0.-.0.0.0.1.-.0.0.1.9.-.c.b.f.6.-.8.d.1.a.7.8.3.a.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.5.9.9.9.7.9.3.0.a.d.5.0.c.9.7.0.a.4.8.1.9.d.0.0.b.5.f.6.d.3.2.4.0.0.0.0.f.f.f.f.!.0.0.0.0.4.6.3.c.4.5.e.1.a.d.c.2.2.6.9.4.5.6.e.1.8.b.6.b.d.4.7.e.5.2.1.5.0.1.d.1.f.5.9.3.!.t.p.y.i.e.n.i.r.b.w.g.p...e.x.e.....T.a.r.g.e.t.A.p.p.V.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_tpyienirbwgp.exe_491668454d7886d02c78a9f3324eec6e9b560bc_bb377917_156a7e34\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):	0.9362570845292987
Encrypted:	false
SSDEEP:	192:VJNOFbaUHY2GWoPjtLIa/u7sFS274ltS:JOBacY2GFPjL/u7sFX4ltS
MD5:	2CBF5D2E716A4E2B5C6D278FE380657F
SHA1:	384DF552BA7C4BCB6AF9CEA2CA8D41C9F7A35C75
SHA-256:	296B9F299B3257C40397466A884CD0192583A8E96E768E42B1159C02C36CB1ED
SHA-512:	9A18CAA5753D47D557BABC07D0FF4D73590B22EF179AD8CBF90D309901F3D794F4A7D615EDE8F1B04A258752B4A486EAF9A7803B36E8A6FCD3AB7F734D181DC6
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.=.1.3.3.2.0.1.9.5.1.4.7.3.1.1.0.2.2.9.....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.=.1.3.3.2.0.1.9.5.1.4.8.4.5.1.6.6.6.3.....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.=.4.a.b.6.0.4.e.0.-.f.e.9.9.-.4.0.7.8.-.8.3.b.1.-.7.3.8.6.7.4.3.8.2.9.2.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.2.5.4.e.f.8.5.-.0.c.8.0.-.4.6.2.2.-.b.e.4.8.-.a.4.a.0.9.4.c.1.a.f.d.2.....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.=.t.p.y.i.e.n.i.r.b.w.g.p...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.5.4.-.0.0.0.1.-.0.0.1.9.-.1.6.b.6.-.9.9.1.5.7.8.3.a.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.5.9.9.9.7.9.3.0.a.d.5.0.c.9.7.0.a.4.8.1.9.d.0.0.b.5.f.6.d.3.2.4.0.0.0.0.f.f.f.f.!.0.0.0.0.4.6.3.c.4.5.e.1.a.d.c.2.2.6.9.4.5.6.e.1.8.b.6.b.d.4.7.e.5.2.1.5.0.1.d.1.f.5.9.3.!.t.p.y.i.e.n.i.r.b.w.g.p...e.x.e.....T.a.r.g.e.t.A.p.p.V.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Feb 6 22:12:27 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	40600
Entropy (8bit):	1.9089113720969164
Encrypted:	false
SSDEEP:	96:5q8GF8v/U/Ah+YSWsVnQH5mFC8cTi72icnus9ikoOuFJwQcv/DhP8st2S+OzbBPI:HLuAcPWsVQszCO2iQJNPzBPbrmsBmw7W
MD5:	524916739B17C605C2740855D1E7EC09
SHA1:	82283EE20177E916CDDCDA1AB1D044DEE085ED18
SHA-256:	53AB2B99083581BDC2B0F0A67B2E1458CE34B129E0FA4EF5D5604E956F2295C9
SHA-512:	AFF9E00E7827410D569BAE50D45E1A82EBCA1C67E53E89208BFC1181245985EB5F9C6C63C248EFE7BB00D89A3AFD7738F806FB1FBA27CE09C52ACEC8AC8AA211
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....K{.c.....\-.....T.....8.....T.....U.....B..... .....GenuineIntelW.....T.....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\WER756B.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):	8368
Entropy (8bit):	3.690412367634023
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiy46O6YBSDSUfgmfjSzo2CpDo89bDYsfohm:RrlsNit6O6YB2SUfgmfjSszDLfT
MD5:	69B0AF479D657FA1AAB1F5B1D5D8A6B3
SHA1:	F64ED0D7D6779D2A6836CC4A3978825DC198D0A7
SHA-256:	ADB3A01ABACCDEBF58B337E58D3A4037125DD6783878C2118AF5FFC690EA2BE8
SHA-512:	6282615E7949977026F11FA8BDB42E396D20ACAC5DFFA8F4ED917027F4B4C1D5F1FDF47AEB97720BEB77985D8DFF70EA797E0902FDED85483EAB889B0016F169
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.>.5.7.1.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER75D9.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4678
Entropy (8bit):	4.428640371795023
Encrypted:	false
SSDEEP:	48:cvIwSD8zsCJgtWI9ZlWgc8sqYj68fm8M4JatkFg+q8vJtp/xl9d:uITfQSUgrsqYDJyVKPp/xl9d
MD5:	0443A3F9E4C64F2076E63D871398340F
SHA1:	DF2AA90A48BD110ECA2562CF67A1F259FD2053D3
SHA-256:	C8550EC9C0DD614286C9284299C53AC51A7C0AA5D53092D213A36D7170BA88AB
SHA-512:	56152EB1ACA2F4D37C1532AF2818517619B23502DC8CE13669A699CA7B089433E48E5D1C15197EE39D34DD638152707EC254A15B5C87AAC45D72329204C6D11
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="1901243" />.. <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\WER82C8.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Feb 6 22:12:31 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	44156
Entropy (8bit):	1.878369031530301
Encrypted:	false
SSDEEP:	192:r5dlzYMjVOKpaOhRdc3Eb90iOif7hUOO+HGo:DlWKp9Rdc0bmKf/Go
MD5:	74158FB4A4C5D428524DFA57C800160F
SHA1:	91FD89B3502EBE8AA35D27A485D9E0AF8D2FB845
SHA-256:	68269F2E6CF5C585DA44D8A6E5E817305A803C12566634C500E22FD3A4BF1445
SHA-512:	EE80D93998D256257F44D1A93F78F92D62C62C9CEA65CBB5472809E2BDBB1B2E954128674F73147CF1B764800683337AFE9A799EDC2BA906C9EE6F5AF410B75B8
Malicious:	false
Preview:	MDMP..... .....O{.c...../.....T.....8.....T.....`.....L.....U.....B.....GenuineIntelW.....T..... ...N{.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\WER84BD.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):	8362
Entropy (8bit):	3.6903200268418375
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi2o6n6YBSUSUDgmfjSzo2CpDH89bUisfjv8m:RrlsNip6n6YBBSUDgmfjSsuUhf1
MD5:	E99E5C0BB9E7AD97E9C5EA642B80D6D9
SHA1:	E651F6215134C7A52E51C7707ADEA8F66825ABFF
SHA-256:	A165CD0C9C52EDD8B366FFE6E55E476A33C5E74327197C8B773CBBD966428206
SHA-512:	069B867E69BAFF255261CE33AF1A4A6452212EBF022D117799C7EA4ADF60C14BCEEFB9FC0CD7FFFBF7014E69E2227783E76E3553F8A88CD4E55271AA45840763
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.4.0.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER84EC.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4678
Entropy (8bit):	4.430634465003027
Encrypted:	false
SSDEEP:	48:cvIwSD8zsCJgtWI9ZlWgc8sqYj88fm8M4JatkFg+q8vJt3/xl1d:uITfQSUgrsqYNJyZKP3/xl1d
MD5:	B02A5A7D16E8340BF24765A193DDDC9E
SHA1:	3A95D434E11165CFBF295BF5913A1F3AD6909C35
SHA-256:	C70ABF707A46B301967A1C419BF7D35D0334B68DC007A2D7CC10E710EABF22AA
SHA-512:	F12581E96D7AD20C3C5583A3D7FEDCD1A0C691A128055F96385F910A994BCB7005B80486D7B2E433357F91B081AA587811E50FFA4EB90690FF5559354B318FFD
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1901243" />.. <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\fwbfw.c

Process:	C:\Users\user\Desktop\lb64Iy4W4e.exe
File Type:	data
Category:	dropped
Size (bytes):	8143
Entropy (8bit):	7.188238050975561
Encrypted:	false
SSDEEP:	192:darcitQvArWiPvQcb9RuplmxcX/sCbFn/u/hhgv6LLtNI7ypzV:uCYrNPvQeAmaECbV+m69NI7q
MD5:	347856D905BEEA5827F7395DDD77048D
SHA1:	9D6D5347AE1CF53C2D187398FDB0CAB438F991C9
SHA-256:	66B1F21A3BE5DAFCCFEF6CFEA835A488608FC471E9AC0D559D84CC4858CE683F
SHA-512:	E9BC2FF8EAAA97F2DD39F76BF9C266DFE68CAB1CDA220237D87D020B2E90F8650EF1E66332E18135B8F809914048AA73B2BEC218B1379904E84E0D78C3D654C
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.[WIT.}....i.W.y.R.}.^.y.W.q.....XW..Mc.....\7!.K.y.a..`.....Z...Jo.....\GB.Gg.u.....X.B.Kg.v.....Pp..Nd.w.....\...Ke.}.....Y...Ko.p... ...G8.u....0<..480fP.401Y7a^?X580..D;.g.....A4...Tgn.`...G.X0P0.80..3cg.a.p0..D.`...igen.a..@.b.e.kX.013^3gR7]804p.F8.a.c..q.ad.G<n.`..D2..qb.e...knj..o.00`...)ecXg`Z]^.q .iYXk^OV.}.lZPU.w.`ZE^.q.iY]T.}.mR.R.t.IT.}._\hR.t...R.}.^.y.W.y.R.u.....ZR..Jo....\5$.O

C:\Users\user\AppData\Local\Temp\nsj2A96.tmp

Process:	C:\Users\user\Desktop\lb64Iy4W4e.exe
File Type:	data
Category:	dropped
Size (bytes):	698028
Entropy (8bit):	7.460862363180337
Encrypted:	false
SSDEEP:	12288:57EOGOwPPrn9SfU+7cCxbOXnKO9tWYI0D9bhoK1j/HD03n1zvPF:57AOwPTU8WbGTtWYI0D9bho2D031zvP
MD5:	EF267C2426AD12867472601EE299537D
SHA1:	A7311F5C90CD1F31F5410A810558FB6242DE5A01
SHA-256:	CBC0231A9AD35A20F279FD0E38093D3DFD0DD6FFE6C276FAD5AE945064E539CC
SHA-512:	CC031C7E2DB6D86B7D3AE6311745E228142C33CB1DBE2EB69593C780CC2484DFB2B669ACE9DBCB05E143A389647CD118450A4490971D24A1616AB9B1BB1EB393
Malicious:	false
Preview:	z-.....,.....m.....,.....z-....."..... .....G.....g...j.....2.....7..... ....

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

Process:	C:\Users\user\Desktop\lb64Iy4W4e.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	370176
Entropy (8bit):	6.615303914837989
Encrypted:	false
SSDEEP:	6144:MWYtu0D9bhoKSoj/QED03mc8+z1zQpb+g4ZeMF:MWYI0D9bhoK1j/HD03n1zvPF
MD5:	64517EEC55E1F3C392B63B73D833E5F9
SHA1:	463C45E1ADC2269456E18B6BD47E521501D1F593
SHA-256:	91E93FF76C34BEB61A02F782558C8FF319558B63E008580EB567DD927663E19C
SHA-512:	E14FAF62CAE49174D895C6552E40FA54038BF46B350C6799938129E60F487F226260A5E3C23996BAF466494D5713A01612454F8C2334E581730CE5C1AE4A56A0
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 23% • Antivirus: Virustotal, Detection: 29%, Browse

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%..a..a..a.....k.....u.....r.....B.....s.....v..a.....`...Y.`.....`..Rich a.....PE..L.....c.....V,.....@.....@.....@z.....0$...h.....h..@.....|..... .....text...+..... ..`.rdata.....@..@.data.....r.....@....gfids.....|.....@..@.rsrc.....~.....@..@.reloc..0$. .....&.....@..B..... .....

C:\Users\user\AppData\Local\Temp\tqtdb.c

Process:	C:\Users\user\Desktop\lb64ly4W4e.exe
File Type:	data
Category:	dropped
Size (bytes):	308051
Entropy (8bit):	7.986580869538692
Encrypted:	false
SSDEEP:	6144:blfN7EA/J3IlnuTtuZd5BCkrSa195056sU+OwHu7sdkwb/mXY:X7EOGOwPPrn9SfU+7cCxbOXY
MD5:	12A293C8002A21714974ED14512456C4
SHA1:	5CFDA98DDB30ED52F34740D33B8197B3447C71A5
SHA-256:	30158501D83CB7C1453D281A51B6F192695E03EE5C90E0642B3EA273FE10BAAA
SHA-512:	C29B0E3F084E170665196E0E2D1D137F5376D8ECAC8BB786BFCB314DCCA6E9B91D3BD408C0F2CD4B165E4184E7FA5CB057C823E3313B71766B07B21BA5DB2I 3E
Malicious:	false
Preview:	.<.Rw.....7... .J...J!....R.F&.....I.J./..O./.kN... .#.;..>e.E./.F...`7.*..]p./.3D..Z6.....}...=.@w*I...g-....:..n.K...<...e.Y(R`*p.V....^.....dL....W.dXz. ..2+*.a.G..l....j...FJ.{.'..:.....g WIr.M .nO.;.[..I..J.....t..@E..P.h.....w..N.....|..J.J...^!..;..~I..p...I(../..O...kN... `#.L..>.../...hX..<...7.8....W..D#I.|G.v_p(lr[..V.[VW...s4.u....nSK...h.H.....~.....(;.Ws@.....~.)0z..... {7...ACG...T7.\....U.U5p.[9_Y..e...h...(.bPVw.x.}...r..7.s..&....z.0..M.(m..P.h...p...uw...*...|...z .J...^!....R.F&.5..v|..e.d.O]..kN... .#.L..>.P../a..zX.....g'#c..W1..D#;.|G_v_.~.)[.}V ..VW...sm.u.Vop.sK....H..;..A...(;k.s!.'.....)Iz.....{7...AC&...k7.\....U.U5p.[9_Y..e...h....7b/Vw.x.}...r....s/3.&....z.0..M.(m..P.h.....w..!....0.... .J...^!....R.F&.....I.J./..O./.kN... .#.L.. >.P../a..zX..<.....8....W.#.D#..|G.v_.(l)[.]V..VW...s4.u....n.K...h.H.....(;k.s!.'.....~.)0z.....{7...AC&...k7.\....U.U5p.[9_Y..e...h....7b/Vw.x.}...r....s/3.&

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

Process:	C:\Users\user\AppData\Local\Temp\tohjyweui.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\tohjyweui.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:s5tn:At
MD5:	51FACF24B75B12CFB8F7B2FB57DA4C58
SHA1:	348477F51F4AA4EF999B743333CE5FDECCF76FB2
SHA-256:	C3AC357375B798C399E6BEF38CD7C254246A6EAB64B0FFF5C163CE385607568C
SHA-512:	B3812D6378CBA61C5504166B2997026494AE6513EA0F56E7952E97BAC8AAA6639359F72B680097714ED5E0F4495B95913B32F6EE39E3F1B0E5D4785758E3CF7F
Malicious:	**true**
Preview:	...3...H

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

Process:	C:\Users\user\AppData\Local\Temp\tohjyweui.exe
File Type:	data

Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44F8
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

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

Process:	C:\Users\user\AppData\Local\Temp\tohjyweui.exe
File Type:	data
Category:	dropped
Size (bytes):	426840
Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC5377612128311076 46ED72B8ED017E7477E600BC0137EF857AE2C
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=..:...L.g<.....I..%4[.G^.~.l'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`'].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...."..bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9..j%..g&....g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\swschqavfbk\tpyienirbwgp.exe

Process:	C:\Users\user\AppData\Local\Temp\tohjyweui.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	370176
Entropy (8bit):	6.615303914837989
Encrypted:	false
SSDEEP:	6144:MWYtu0D9bhoKSoj/QED03mc8+z1zQpb+g4ZeMF:MWYl0D9bhoK1j/HD03n1zvPF
MD5:	64517EEC55E1F3C392B63B73D833E5F9
SHA1:	463C45E1ADC2269456E18B6BD47E521501D1F593
SHA-256:	91E93FF76C34BEB61A02F782558C8FF319558B63E008580EB567DD927663E19C
SHA-512:	E14FAF62CAE49174D895C6552E40FA54038BF46B350C6799938129E60F487F226260A5E3C23996BAF466494D5713A01612454F8C2334E581730CE5C1AE4A56A0
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 23%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%..a..a..a.....k.....u.....r.....B.....s.....v..a.....`...Y.`.....`..Richa.....PE..L.....c.....V,.....@.....@.....@.....@z.....0$...h.....h..@.....|.....text...+..... ..`.rdata.....@..@.data.....r.....@....gfids.....|.....@..@.rsrc.....~.....@..@.reloc..0$.....&.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.396277761181723

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:	lb64Iy4W4e.exe
File size:	663392
MD5:	4c7df43e37814754ad1c8a97ab971af8
SHA1:	c2315cba4dc175554869cf1c7d7b4ddfdb65adea
SHA256:	49cc6f25d16cf7c85d218bcd4ecbdedce0f5d4540bc5099436511291f48a3976
SHA512:	635c6f4c3d20a691cadae02d8f857d6aa37775b1d55302c59498e0ace80152413be2f0fd22b328db96ed41e381868f9c026f5176b430ba5e969dba8347f3d8a3
SSDEEP:	12288:3YueB8OT4Q9HIbbir1vIm4KQH/HxCl9KOlOMyhiZq+zeRZA7Y1g9R:3YPT4Q9HHr1vIRCLShqq+FL
TLSH:	74E402247A10C56FCA905BB84EA5E3B457B0EE5D3E549F0B63E03FBFBDB91915908220
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:	f2d29cccdcdcccdc

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

Instruction
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 00007FAD50A616FAh
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FAD50A616CAh
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	0x32e60	.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	0x32e60	0x33000	False	0.4702914368872549	data	5.337142337075559	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b358	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584	English	United States
RT_ICON	0x4bb80	0xaac8	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x56648	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 38016	English	United States
RT_ICON	0x5faf0	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 21600	English	United States
RT_ICON	0x64f78	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896	English	United States
RT_ICON	0x691a0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x6b748	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x6c7f0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	United States
RT_ICON	0x6d178	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_DIALOG	0x6d5e0	0x100	data	English	United States
RT_DIALOG	0x6d6e0	0x11c	data	English	United States
RT_DIALOG	0x6d800	0x60	data	English	United States
RT_GROUP_ICON	0x6d860	0x84	data	English	United States
RT_VERSION	0x6d8e8	0x234	data	English	United States
RT_MANIFEST	0x6db20	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

DLL	Import
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
192.168.2.545.132.106.37 4971264452816766 02/06/23-14:12:55.395066	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49712	6445	192.168.2.5	45.132.106.37
45.132.106.37192.168.2.5 6445497312841753 02/06/23-14:13:52.517965	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49731	45.132.106.37	192.168.2.5
192.168.2.545.132.106.37 4970964452816766 02/06/23-14:12:39.702248	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49709	6445	192.168.2.5	45.132.106.37
45.132.106.37192.168.2.5 6445497072841753 02/06/23-14:12:33.506820	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49707	45.132.106.37	192.168.2.5
192.168.2.545.132.106.37 4973564452816766 02/06/23-14:14:08.694757	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49735	6445	192.168.2.5	45.132.106.37
45.132.106.37192.168.2.5 6445497202841753 02/06/23-14:13:12.771040	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49720	45.132.106.37	192.168.2.5
192.168.2.545.132.106.37 4972964452816766 02/06/23-14:13:42.328059	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49729	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.37 4970264452816766 02/06/23-14:12:20.468192	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49702	6445	192.168.2.5	45.132.106.37
45.132.106.37192.168.2.5 6445497252841753 02/06/23-14:13:29.137140	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49725	45.132.106.37	192.168.2.5
192.168.2.545.132.106.37 4971164452823337 02/06/23-14:12:50.979729	TCP	2823337	ETPRO TROJAN Nanocore Checkin Pattern	49711	6445	192.168.2.5	45.132.106.37
45.132.106.37192.168.2.5 6445497202810451 02/06/23-14:13:12.771040	TCP	2810451	ETPRO TROJAN NanoCore RAT Keepalive Response 3	6445	49720	45.132.106.37	192.168.2.5
45.132.106.37192.168.2.5 6445497332841753 02/06/23-14:13:57.153095	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49733	45.132.106.37	192.168.2.5

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
45.132.106.37192.168.2.56445497352841753 02/06/23-14:14:08.617792	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49735	45.132.106.37	192.168.2.5
45.132.106.37192.168.2.56445497362841753 02/06/23-14:14:13.470154	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49736	45.132.106.37	192.168.2.5
192.168.2.545.132.106.374972264452816766 02/06/23-14:13:18.836838	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49722	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.374971664452816766 02/06/23-14:12:59.871071	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49716	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.374970364452816766 02/06/23-14:12:29.256960	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.374972664452816766 02/06/23-14:13:33.513858	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49726	6445	192.168.2.5	45.132.106.37
45.132.106.37192.168.2.56445497272841753 02/06/23-14:13:37.915437	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49727	45.132.106.37	192.168.2.5
45.132.106.37192.168.2.56445497292841753 02/06/23-14:13:42.158315	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49729	45.132.106.37	192.168.2.5
45.132.106.37192.168.2.56445497022841753 02/06/23-14:12:20.379177	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49702	45.132.106.37	192.168.2.5
45.132.106.37192.168.2.56445497262841753 02/06/23-14:13:33.469565	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49726	45.132.106.37	192.168.2.5
192.168.2.545.132.106.374973364452816766 02/06/23-14:13:57.290193	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49733	6445	192.168.2.5	45.132.106.37
45.132.106.37192.168.2.56445497012841753 02/06/23-14:12:15.717836	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49701	45.132.106.37	192.168.2.5
192.168.2.545.132.106.374970764452816766 02/06/23-14:12:33.686837	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49707	6445	192.168.2.5	45.132.106.37
45.132.106.37192.168.2.56445497122841753 02/06/23-14:12:55.336364	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49712	45.132.106.37	192.168.2.5
45.132.106.37192.168.2.56445497162841753 02/06/23-14:12:59.766454	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49716	45.132.106.37	192.168.2.5
45.132.106.37192.168.2.56445497192841753 02/06/23-14:13:08.445515	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49719	45.132.106.37	192.168.2.5
192.168.2.545.132.106.374972364452816766 02/06/23-14:13:24.891407	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49723	6445	192.168.2.5	45.132.106.37
45.132.106.37192.168.2.56445497172841753 02/06/23-14:13:04.143032	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49717	45.132.106.37	192.168.2.5
45.132.106.37192.168.2.56445497112841753 02/06/23-14:12:50.916490	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6445	49711	45.132.106.37	192.168.2.5

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.545.132.106.37 4971764452816766 02/06/23-14:13:04.199805	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49717	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.37 4972764452816766 02/06/23-14:13:37.920388	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49727	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.37 4973064452816766 02/06/23-14:13:48.218570	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49730	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.37 4972264452816718 02/06/23-14:13:18.233724	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49722	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.37 4973464452816766 02/06/23-14:14:04.014579	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49734	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.37 4971064452816766 02/06/23-14:12:46.639827	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49710	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.37 4972064452816766 02/06/23-14:13:12.842490	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49720	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.37 4971164452816766 02/06/23-14:12:50.979729	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49711	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.37 4973164452816766 02/06/23-14:13:52.687469	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49731	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.37 4970164452816766 02/06/23-14:12:15.779461	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49701	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.37 4972564452816766 02/06/23-14:13:29.249183	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49725	6445	192.168.2.5	45.132.106.37
45.132.106.37192.168.2.5 6445497092810290 02/06/23-14:12:38.309927	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	6445	49709	45.132.106.37	192.168.2.5
192.168.2.545.132.106.37 4971964452816766 02/06/23-14:13:08.627802	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49719	6445	192.168.2.5	45.132.106.37
192.168.2.545.132.106.37 4970364452816718 02/06/23-14:12:27.309652	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49703	6445	192.168.2.5	45.132.106.37

Network Port Distribution

Total Packets: 70

- 53 (DNS)
- 6445 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 6, 2023 14:12:15.550626040 CET	49701	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:15.580632925 CET	6445	49701	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:15.580776930 CET	49701	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:15.631295919 CET	49701	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:15.676197052 CET	6445	49701	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:15.687864065 CET	49701	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:15.717835903 CET	6445	49701	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:15.718019962 CET	49701	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:15.747594118 CET	6445	49701	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:15.779460907 CET	49701	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:15.858882904 CET	6445	49701	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:15.863033056 CET	49701	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:15.943516970 CET	49701	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:15.952651978 CET	6445	49701	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:15.953249931 CET	49701	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:20.210206985 CET	49702	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:20.239721060 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.239864111 CET	49702	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:20.258255005 CET	49702	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:20.316607952 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.316914082 CET	49702	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:20.349812031 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.349951982 CET	49702	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:20.379177094 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.379296064 CET	49702	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:20.468054056 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.468192101 CET	49702	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:20.501760006 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.501795053 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.501815081 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.501837015 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.501878977 CET	49702	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:20.501914978 CET	49702	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:20.526129007 CET	49702	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:20.530669928 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.530744076 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.530775070 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.530891895 CET	49702	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:20.531017065 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.531049013 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.531078100 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.531106949 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.531137943 CET	6445	49702	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:20.531161070 CET	49702	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:20.531184912 CET	49702	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:26.676229000 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:26.714061975 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:26.714267015 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:26.753952026 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:26.827461004 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:26.827663898 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:26.921391964 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:26.921576023 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:26.950916052 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:26.962414026 CET	49703	6445	192.168.2.5	45.132.106.37

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 6, 2023 14:12:27.046224117 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.046386003 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.076018095 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.076051950 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.076072931 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.076097965 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.076158047 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.076158047 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.086903095 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.105926991 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.106000900 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.106045961 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.106076956 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.106089115 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.106117964 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.106117964 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.106132984 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.106154919 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.106177092 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.106189013 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.106220961 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.106235981 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.106266022 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.106276989 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.106332064 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.135333061 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.135390043 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.135423899 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.135458946 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.135481119 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.135489941 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.135513067 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.135521889 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.135560989 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.135591030 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.135591984 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.135613918 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.135637045 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.135668039 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.135680914 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.135699034 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.135731936 CET	6445	49703	45.132.106.37	192.168.2.5
Feb 6, 2023 14:12:27.135735035 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.135747910 CET	49703	6445	192.168.2.5	45.132.106.37
Feb 6, 2023 14:12:27.135765076 CET	6445	49703	45.132.106.37	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 6, 2023 14:12:15.426714897 CET	61893	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:12:15.533972979 CET	53	61893	8.8.8.8	192.168.2.5
Feb 6, 2023 14:12:20.100056887 CET	60649	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:12:20.208462000 CET	53	60649	8.8.8.8	192.168.2.5
Feb 6, 2023 14:12:24.860294104 CET	51441	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:12:24.969638109 CET	53	51441	8.8.8.8	192.168.2.5
Feb 6, 2023 14:12:33.325907946 CET	61452	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:12:33.434902906 CET	53	61452	8.8.8.8	192.168.2.5
Feb 6, 2023 14:12:37.797481060 CET	65323	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:12:37.817137957 CET	53	65323	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 6, 2023 14:12:43.868993998 CET	51484	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:12:43.889022112 CET	53	51484	8.8.8.8	192.168.2.5
Feb 6, 2023 14:12:50.823187113 CET	63446	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:12:50.841149092 CET	53	63446	8.8.8.8	192.168.2.5
Feb 6, 2023 14:12:55.152124882 CET	56751	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:12:55.259871006 CET	53	56751	8.8.8.8	192.168.2.5
Feb 6, 2023 14:12:59.525441885 CET	55068	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:12:59.635647058 CET	53	55068	8.8.8.8	192.168.2.5
Feb 6, 2023 14:13:04.046624899 CET	56682	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:13:04.065140009 CET	53	56682	8.8.8.8	192.168.2.5
Feb 6, 2023 14:13:08.351641893 CET	62659	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:13:08.369720936 CET	53	62659	8.8.8.8	192.168.2.5
Feb 6, 2023 14:13:12.673418999 CET	58581	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:13:12.691442966 CET	53	58581	8.8.8.8	192.168.2.5
Feb 6, 2023 14:13:17.034033060 CET	65513	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:13:17.052063942 CET	53	65513	8.8.8.8	192.168.2.5
Feb 6, 2023 14:13:22.955478907 CET	56687	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:13:23.066755056 CET	53	56687	8.8.8.8	192.168.2.5
Feb 6, 2023 14:13:29.044564962 CET	52688	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:13:29.064649105 CET	53	52688	8.8.8.8	192.168.2.5
Feb 6, 2023 14:13:33.371251106 CET	61344	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:13:33.389108896 CET	53	61344	8.8.8.8	192.168.2.5
Feb 6, 2023 14:13:37.719351053 CET	53972	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:13:37.826854944 CET	53	53972	8.8.8.8	192.168.2.5
Feb 6, 2023 14:13:42.069423914 CET	58472	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:13:42.087323904 CET	53	58472	8.8.8.8	192.168.2.5
Feb 6, 2023 14:13:46.482965946 CET	60177	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:13:46.501174927 CET	53	60177	8.8.8.8	192.168.2.5
Feb 6, 2023 14:13:52.392618895 CET	60284	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:13:52.412906885 CET	53	60284	8.8.8.8	192.168.2.5
Feb 6, 2023 14:13:56.955427885 CET	50902	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:13:57.066534042 CET	53	50902	8.8.8.8	192.168.2.5
Feb 6, 2023 14:14:01.363904953 CET	53823	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:14:01.702450037 CET	53	53823	8.8.8.8	192.168.2.5
Feb 6, 2023 14:14:08.415575981 CET	49769	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:14:08.523582935 CET	53	49769	8.8.8.8	192.168.2.5
Feb 6, 2023 14:14:13.383150101 CET	49579	53	192.168.2.5	8.8.8.8
Feb 6, 2023 14:14:13.401088953 CET	53	49579	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 6, 2023 14:12:15.426714897 CET	192.168.2.5	8.8.8.8	0x65bc	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:20.100056887 CET	192.168.2.5	8.8.8.8	0xff1	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:24.860294104 CET	192.168.2.5	8.8.8.8	0x37d5	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:33.325907946 CET	192.168.2.5	8.8.8.8	0x815	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:37.797481060 CET	192.168.2.5	8.8.8.8	0xc389	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:43.868993998 CET	192.168.2.5	8.8.8.8	0x1b3f	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:50.823187113 CET	192.168.2.5	8.8.8.8	0xf6f0	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:55.152124882 CET	192.168.2.5	8.8.8.8	0xc366	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:59.525441885 CET	192.168.2.5	8.8.8.8	0x24a0	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:04.046624899 CET	192.168.2.5	8.8.8.8	0x8593	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 6, 2023 14:13:08.351641893 CET	192.168.2.5	8.8.8.8	0x44d3	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:12.673418999 CET	192.168.2.5	8.8.8.8	0x4bc6	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:17.034033060 CET	192.168.2.5	8.8.8.8	0x77f3	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:22.955478907 CET	192.168.2.5	8.8.8.8	0xd47b	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:29.044564962 CET	192.168.2.5	8.8.8.8	0x4e86	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:33.371251106 CET	192.168.2.5	8.8.8.8	0xde45	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:37.719351053 CET	192.168.2.5	8.8.8.8	0xadce	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:42.069423914 CET	192.168.2.5	8.8.8.8	0xee19	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:46.482965946 CET	192.168.2.5	8.8.8.8	0x1898	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:52.392618895 CET	192.168.2.5	8.8.8.8	0x665c	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:56.955427885 CET	192.168.2.5	8.8.8.8	0xc871	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:14:01.363904953 CET	192.168.2.5	8.8.8.8	0x26a	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:14:08.415575981 CET	192.168.2.5	8.8.8.8	0xd10c	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:14:13.383150101 CET	192.168.2.5	8.8.8.8	0xa53f	Standard query (0)	alertt.duckdns.org	A (IP address)	IN (0x0001)	false

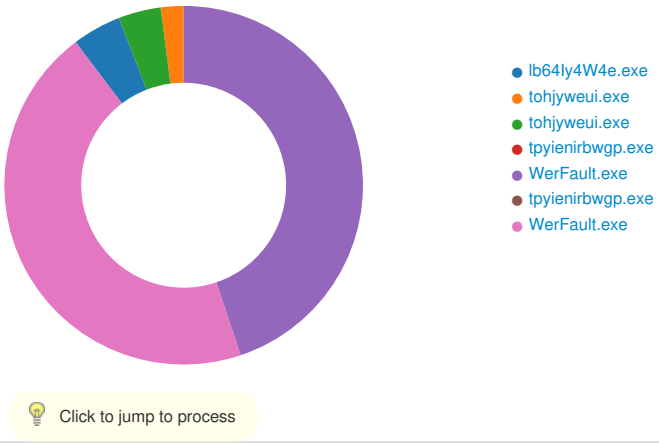
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 6, 2023 14:12:15.533972979 CET	8.8.8.8	192.168.2.5	0x65bc	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:20.208462000 CET	8.8.8.8	192.168.2.5	0xff1	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:24.969638109 CET	8.8.8.8	192.168.2.5	0x37d5	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:33.434902906 CET	8.8.8.8	192.168.2.5	0x815	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:37.817137957 CET	8.8.8.8	192.168.2.5	0xc389	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:43.889022112 CET	8.8.8.8	192.168.2.5	0x1b3f	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:50.841149092 CET	8.8.8.8	192.168.2.5	0xf6f0	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:55.259871006 CET	8.8.8.8	192.168.2.5	0xc366	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:12:59.635647058 CET	8.8.8.8	192.168.2.5	0x24a0	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:04.065140009 CET	8.8.8.8	192.168.2.5	0x8593	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:08.369720936 CET	8.8.8.8	192.168.2.5	0x44d3	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:12.691442966 CET	8.8.8.8	192.168.2.5	0x4bc6	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:17.052063942 CET	8.8.8.8	192.168.2.5	0x77f3	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 6, 2023 14:13:23.066755056 CET	8.8.8.8	192.168.2.5	0xd47b	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:29.064649105 CET	8.8.8.8	192.168.2.5	0x4e86	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:33.389108896 CET	8.8.8.8	192.168.2.5	0xde45	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:37.826854944 CET	8.8.8.8	192.168.2.5	0xadce	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:42.087323904 CET	8.8.8.8	192.168.2.5	0xee19	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:46.501174927 CET	8.8.8.8	192.168.2.5	0x1898	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:52.412906885 CET	8.8.8.8	192.168.2.5	0x665c	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:13:57.066534042 CET	8.8.8.8	192.168.2.5	0xc871	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:14:01.702450037 CET	8.8.8.8	192.168.2.5	0x26a	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:14:08.523582935 CET	8.8.8.8	192.168.2.5	0xd10c	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false
Feb 6, 2023 14:14:13.401088953 CET	8.8.8.8	192.168.2.5	0xa53f	No error (0)	alertt.duckdns.org		45.132.106.37	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: lb64ly4W4e.exe PID: **4332**, Parent PID: **3324**

General

Target ID:	0
Start time:	14:12:08

Start date:	06/02/2023
Path:	C:\Users\user\Desktop\lb64ly4W4e.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\lb64ly4W4e.exe
Imagebase:	0x400000
File size:	663392 bytes
MD5 hash:	4C7DF43E37814754AD1C8A97AB971AF8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsj2A95.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsj2A96.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nse2AC6.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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nse2AC6.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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\tqtdb.c	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\fwbfw.c	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\tohjyweui.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\nsj2A95.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nse2AC6.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\nsj2A96.tmp	0	26629	7a 2d 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 02 00 00 00 fd 11 00 00 6d 00 00 00 fd 1d 00 00 00 00 00 00 fd 2c 00 00 01 00 00 00 7a 2d 00 00 00 00 00 00 00 00 00 00 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 22 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	z-,m,z-"	success or wait	35	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tqtdb.c	0	16384	fd 3c fd 52 77 01 fd 0c fd fd fd fd 37 fd fd 81 20 fd 4a 13 05 fd 4a 21 fd fd fd fd 52 fd 46 26 06 fd fd fd 2e 49 fd 4a 1e 2f 09 fd 4f fd 2f 1c 6b 4e fd 1d fd 20 0d 23 fd 3b fd fd 3e 65 fd 45 04 2f fd 46 01 fd fd 60 37 00 2a fd fd 5d 70 33 2f 1e 33 44 fd fd 5a 36 fd fd fd 75 fd 7d fd 0e fd 3d f4 40 77 2a 49 fd fd fd 67 2d fd fd fd fd 3a fd fd 6e fd 4b fd fe fd 3c fd fd fd 65 fd 59 28 52 60 2a 70 fd 56 fd 19 36 fd 5e fd 02 1c fd fd 64 4c fd 00 01 fd 57 fd 64 58 7a fd 20 fd 25 32 2b 2a fd 61 3b 47 fd fd 6c fd 18 fd fd 6a fd fd 16 46 4a fd 7b fd 27 12 fd 3a fd 01 fd 16 03 fd fd fd fd fd fd 15 67 57 49 72 fd 4d 20 f7 6e 4f fd 3b fd 5b fd fd 49 fd fd 4a fd 08 fd 10 fd ed 74 fd fd 40 45 fd fd 50 fd 68 dd fd	<Rw7 JJ!RF&.IJ/O/kN #;>eE/F`7* ]p/3DZ6}=@w*Ig- :nK<eY(R`*pV^dLWdXz 2+*aGljFJ{':gWIrM nO;[IJt @EPh	success or wait	19	406224	WriteFile
C:\Users\user\AppData\Local\Temp\fwbfw.c	0	8143	e3 37 30 35 6d fd 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 $A5=<r	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\tohjyweui.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 25 fd 1e 61 26 fd 61 26 fd 61 26 45 fd fd fd 6b 26 45 fd fd fd fd 26 45 fd fd fd 75 26 fd 0e fd fd 72 26 fd 0e fd fd 42 26 fd 0e fd fd 73 26 45 fd fd fd 76 26 fd 61 27 fd fd 26 fd 0e fd fd 60 26 fd 0e 59 fd 60 26 fd 0e fd fd 60 26 fd 52 69 63 68 61 26 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06	MZ@!L!This program cannot be run in DOS mode.$%aaakurBsva`Y` `RichaPEL	success or wait	23	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\lb64Iy4W4e.exe	unknown	512	success or wait	476	4061F5	ReadFile
C:\Users\user\Desktop\lb64Iy4W4e.exe	unknown	16384	success or wait	26	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsj2A96.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsj2A96.tmp	unknown	11642	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsj2A96.tmp	unknown	4	success or wait	3	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsj2A96.tmp	unknown	16384	success or wait	43	4061F5	ReadFile

Analysis Process: tohjyweui.exe PID: **5884**, Parent PID: **4332**

General

Target ID:	1
Start time:	14:12:08
Start date:	06/02/2023
Path:	C:\Users\user\AppData\Local\Temp\tohjyweui.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\tohjyweui.exe" C:\Users\user\AppData\Local\Temp\fwbfw.c
Imagebase:	0x9b0000
File size:	370176 bytes
MD5 hash:	64517EEC55E1F3C392B63B73D833E5F9
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: 00000001.00000002.320288694.0000000000630000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.320288694.0000000000630000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.320288694.0000000000630000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.320288694.0000000000630000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.320288694.0000000000630000.00000004.00001000.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.320288694.0000000000630000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 23%, ReversingLabs • Detection: 29%, Virustotal, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\swschqavfbk	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	600414	CreateDirectoryW
C:\Users\user\AppData\Roaming\swschqavfbk\tpyienirbwgp.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	600357	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\swschqavfbk\tpyienirbwgp.exe	0	370176	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 25 fd 1e 61 26 fd 61 26 fd 61 26 45 fd fd fd 6b 26 45 fd fd fd fd 26 45 fd fd fd 75 26 fd 0e fd fd 72 26 fd 0e fd fd 42 26 fd 0e fd fd 73 26 45 fd fd fd 76 26 fd 61 27 fd fd 26 fd 0e fd fd 60 26 fd 0e 59 fd 60 26 fd 0e fd fd 60 26 fd 52 69 63 68 61 26 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06	MZ@!L!This program cannot be run in DOS mode.$%aaakurBsva`Y` `RichaPEL	success or wait	1	600366	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fwbfw.c	unknown	4096	success or wait	1	9E2FB0	ReadFile
C:\Users\user\AppData\Local\Temp\fwbfw.c	unknown	4096	success or wait	1	9E2FB0	ReadFile
C:\Users\user\AppData\Local\Temp\tohjyweui.exe	unknown	370176	success or wait	1	600339	ReadFile
C:\Users\user\AppData\Local\Temp\tqtdb.c	unknown	287232	success or wait	1	601238	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6017F0	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6017F0	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6017F0	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6017F0	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6017F0	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6017F0	ReadFile

Registry Activities

Analysis Process: tohjyweui.exe

PID: **4560**, Parent PID: **5884**

General

Target ID:	2
Start time:	14:12:10
Start date:	06/02/2023
Path:	C:\Users\user\AppData\Local\Temp\tohjyweui.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\tohjyweui.exe
Imagebase:	0x9b0000
File size:	370176 bytes
MD5 hash:	64517EEC55E1F3C392B63B73D833E5F9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6B9F60AC	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	6B9F60AC	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	5820F79	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	5821073	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	5820F79	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	5820F79	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6B9F60AC	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	6B9F60AC	unknown
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	5821073	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	5821073	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	5821073	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 11 fd 33 fd 08 fd 48	3H	success or wait	1	582122B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	21	582122B	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	426840	fd fd 67 26 6a 6f 1f 01 fd 49 50 67 08 fd 62 47 4d 64 fd 0d fd 52 3e 69 fd fd 09 6f fd fd 04 49 fd 3e f0 26 fd 72 7b fd fd fd fd 38 fd e5 fd 7d fd 89 fd 45 03 7f fd fd 76 fd 21 37 fd 75 33 65 fd fd 20 fd fd 05 fd fd 64 62 fd fd 15 7d fd fd 1d 02 02 fd fd 22 fd 74 28 06 78 43 39 fd 63 70 15 42 fd fd fd fd 37 fd 0f 1b 27 fd fd fd fd fd 7f fd 25 fd 09 fd 06 fd fd 77 fd 5e fd fd 5f 13 fd fd 02 1d 34 fd 42 fd 57 25 fd 3c a6 64 69 fd 30 fd 7b 39 fd 78 53 fd fd fd 35 fd fd fd 29 05 fd 77 fd 0f 24 14 fd 43 fd fd 3f 60 46 cf fd 75 fd 35 d2 54 fd 58 fd 77 27 53 69 fd fd 7a fd 6e 7b fd fd c4 59 21 6d fd fd 1c 52 41 fd fd fd 78 67 fd 3a 03 fd 5b 37 fd 18 fd 7a fd fd 39 40 02 4b fd 2d fd fd fd 54 fd fd 2b fd 41 43 65	g&joIPgGMR>ioI>&r{8}E v!7u3e db }"t(xC9cpB7'%w^_BW% <i0{9xS5)w$C? `Fu5TXw'Sizn{Y!mRAxg[7z9@K-T+ACe	success or wait	1	582122B	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	582122B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6BA25544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6BA25544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6BA28738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6BA25544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	4	6BA25544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	6BA25544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	582122B	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6BACBF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6BACBF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6BACBF06	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6BACBF06	unknown

Analysis Process: tpyienirbwgp.exe PID: **5716**, Parent PID: **3324**

General

Target ID:	3
Start time:	14:12:21
Start date:	06/02/2023
Path:	C:\Users\user\AppData\Roaming\swschqavfbk\tpyienirbwgp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\swschqavfbk\tpyienirbwgp.exe" "C:\Users\user\AppData\Local\Temp\tohjyweui.exe" C:\Users\user\A
Imagebase:	0x990000
File size:	370176 bytes
MD5 hash:	64517EEC55E1F3C392B63B73D833E5F9
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 23%, ReversingLabs
Reputation:	low

Analysis Process: WerFault.exe PID: **5420**, Parent PID: **5716**

General

Target ID:	6
Start time:	14:12:26
Start date:	06/02/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5716 -s 632
Imagebase:	0x890000
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	68DB1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	68DA497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER75D9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER75D9.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	68DA497A	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_tpyienirbwgp.exe_491668454d7886d02c78a9f3324eec6e9b560bc_bb377917_156a7e34	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_tpyienirbwgp.exe_491668454d7886d02c78a9f3324eec6e9b560bc_bb377917_156a7e34\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	68DA497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER75D9.tmp	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER75D9.tmp.xml	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER75F6.tmp.csv	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER76F1.tmp.txt	success or wait	1	68DA497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 4b 7b fd 63 fd 05 12 00 00 00 00 00	MDMP K{c	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	7456	6	00 00 00 00 00 00		success or wait	1	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 20 1d 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 54 16 00 00 45 7b 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	UB GenuineIntelWTTE{c Pacific Standard TimePacific Daylight Time	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	8748	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 2f 01 00 00 00 00 30 fd 6d 76 fd 01 00 00 05 00 00 00 01 00 00 00 fd fd 2f 01 fd 1b 00 23 00 00 00 02 02 00 00 70 fd 2f 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++/0mv/#p/+	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	1620	168	20 16 00 00 00 00 00 00 09 04 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 fd 1b 00 00 00 00 00 01 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 2c 22 00 00	,"	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	11612	20	0e 00 00 00 60 6a 40 01 00 00 00 00 04 00 00 00 40 2e 00 00	`j@@.	success or wait	14	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	11840	4	14 12 09 77	w	success or wait	13	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	29540	2064	fd fd 0f 77 fd fd 0d 77 fd 00 00 00 fd fd fd fd 10 00 00 00 fd fd 6c 01 50 fd 6c 01 fd fd fd fd 40 fd 0d 77 40 fd 0d 77 fd fd fd fd 00 fd 07 01 00 fd 07 01 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd 07 01 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 6e 40 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 60 48 41 01 00 00 00 00 00 00 00 00 60 6a 40 01 00 40 07 01 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 01 54 42 07 01 fd fd fd 01 fd 6e 40 01 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwlPl@w@wn@`HA`j@ @TBn@	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	1788	4	03 00 00 00		success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	9464	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd 2f 01 00 00 00 00 30 fd 6d 76 fd 01 00 00 fd fd fd fd fd fd fd fd fd fd 2f 01 fd 1b 00 23 00 00 00 02 02 00 00 70 fd 2f 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++/0mv/#p/+	success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	1888	48	fd 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 07 01 00 00 00 00 1c fd fd 01 00 00 00 00 fd 09 00 00 fd 63 00 00 fd 02 00 00 fd 2a 00 00	c*	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	1948	4	2d 00 00 00	-	success or wait	45	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	7462	38	20 00 00 00 74 00 70 00 79 00 69 00 65 00 6e 00 69 00 72 00 62 00 77 00 67 00 70 00 2e 00 65 00 78 00 65 00 00 00	tpyienirbwgp.exe	success or wait	45	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	6704	752	00 00 3a 73 00 00 00 00 00 00 03 00 fd fd 03 00 fd 2a 2c fd 0e 22 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 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 40 fd 02 00 00 00 00 00 fd 46 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 19 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 18 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 15 67 06 00 00 00 00	:s*,"BB?%@AZb@F@g	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	31604	8996	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7318.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 00 13 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 5c 2d 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 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 1a 00 00 16 00 00 00 fd 00 00 00 fd 1c 00 00	\-T8T	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5716</Pid>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1002	78	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 74 00 70 00 79 00 69 00 65 00 6e 00 69 00 72 00 62 00 77 00 67 00 70 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>tpyienirbwgp.exe</ImageName>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1080	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1084	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1088	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 32 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000002</CmdLineSignature>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1178	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1182	2	09 00		success or wait	2	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1186	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 32 00 30 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6202</Uptime>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1228	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1232	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1236	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1318	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1322	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1326	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1378	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1382	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1386	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1430	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1434	2	09 00		success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1440	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 34 00 36 00 32 00 39 00 38 00 38 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>94629888</PeakVirtualSize>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1536	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 33 00 31 00 32 00 32 00 35 00 36 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>93122560</VirtualSize>	success or wait	1	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1606	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1610	2	09 00		success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1616	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 31 00 33 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>2135</PageFaultCount>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1690	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1694	2	09 00		success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1700	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 38 00 32 00 34 00 35 00 32 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>8245248</PeakWorkingSetSize>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1796	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1800	2	09 00		success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1806	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 38 00 32 00 34 00 35 00 32 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>8245248</WorkingSetSize>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1886	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1890	2	09 00		success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	1896	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 39 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>179984</QuotaPeakPagedPoolUsage>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2010	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2014	2	09 00		success or wait	3	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2020	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 38 00 38 00 30 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>178800</QuotaPagedPoolUsage>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2118	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2122	2	09 00		success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2128	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 36 00 31 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>22616</QuotaPeakNonPagedPoolUsage>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2252	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2256	2	09 00		success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2262	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2370	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2374	2	09 00		success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2380	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 35 00 37 00 31 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1757184</PagefileUsage>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2456	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2460	2	09 00		success or wait	3	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2466	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 36 00 31 00 32 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1761280</PeakPagefileUsage>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2558	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2562	2	09 00		success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2568	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 35 00 37 00 31 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1757184</PrivateUsage>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2640	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2644	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2648	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2694	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2698	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2702	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2732	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2736	2	09 00		success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2742	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2782	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2786	2	09 00		success or wait	4	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2794	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2824	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2828	2	09 00		success or wait	4	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2836	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2906	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2910	2	09 00		success or wait	4	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	2918	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3008	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3012	2	09 00		success or wait	4	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3020	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 36 00 31 00 36 00 36 00 39 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4616692</Uptime>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3068	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3072	2	09 00		success or wait	4	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3080	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3158	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3162	2	09 00		success or wait	4	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3170	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3222	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3226	2	09 00		success or wait	4	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3234	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	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3278	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3282	2	09 00		success or wait	5	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3292	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3382	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3386	2	09 00		success or wait	5	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3396	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3470	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3474	2	09 00		success or wait	5	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3484	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 36 00 39 00 38 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>66989</PageFaultCount>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3560	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3564	2	09 00		success or wait	5	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3574	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 36 00 38 00 35 00 33 00 31 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>126853120</PeakWorkingSetSize>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3674	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3678	2	09 00		success or wait	5	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3688	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 36 00 30 00 31 00 37 00 35 00 33 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>126017536</WorkingSetSize>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3772	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3776	2	09 00		success or wait	5	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3786	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 38 00 30 00 35 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>1180512</QuotaPeakPagedPoolUsage>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3902	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3906	2	09 00		success or wait	5	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	3916	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 31 00 33 00 36 00 36 00 32 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>1136624</QuotaPagedPoolUsage>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4016	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4020	2	09 00		success or wait	5	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4030	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 31 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>91984</QuotaPeakNonPagedPoolUsage>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4154	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4158	2	09 00		success or wait	5	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4168	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 33 00 34 00 37 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>83472</QuotaNonPagedPoolUsage>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4276	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4280	2	09 00		success or wait	5	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4290	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 36 00 33 00 38 00 37 00 32 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>463872000</PagefileUsage>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4368	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4372	2	09 00		success or wait	5	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4382	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 35 00 34 00 32 00 32 00 37 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>47542272</PeakPagefileUsage>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4476	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4480	2	09 00		success or wait	5	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4490	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 36 00 33 00 38 00 37 00 32 00 30 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>46387200</PrivateUsage>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4564	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4568	2	09 00		success or wait	4	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4576	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4632	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4674	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4678	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4682	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4720	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4762	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4766	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4768	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4806	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4810	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4814	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	9	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	18	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	4874	82	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 74 00 70 00 79 00 69 00 65 00 6e 00 69 00 72 00 62 00 77 00 67 00 70 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>tpyienirbwgp.exe</Parameter0>	success or wait	9	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	5560	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	5564	2	09 00		success or wait	1	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	5566	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	5606	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	5610	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	5612	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	5650	4	0d 00 0a 00		success or wait	6	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	5654	2	09 00		success or wait	12	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	5658	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6212	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6216	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6218	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6258	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6262	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6264	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6302	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6306	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6310	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6404	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6408	2	09 00		success or wait	2	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6412	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 6c 00 67 00 6a 00 70 00 72 00 6b 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>lgjprk, Inc.</SystemManufacturer>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6518	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6522	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6526	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 6c 00 67 00 6a 00 70 00 72 00 6b 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>lgjprk7,1</SystemProductName>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6622	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6626	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6630	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6750	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6754	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6758	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 33 00 35 00 38 00 34 00 30 00 32 00 35 00 32 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>1635840252</OSInstallDate>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6840	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6844	2	09 00		success or wait	2	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6848	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6950	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6954	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	6958	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7026	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7030	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7032	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7072	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7076	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7078	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7112	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7116	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7120	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7216	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7220	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7222	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	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7258	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7262	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7264	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7288	4	0d 00 0a 00		success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7292	2	09 00		success or wait	6	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7296	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 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>80000000</Flags>	success or wait	3	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7542	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7546	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7548	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7574	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7578	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7580	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 36 00 54 00 32 00 32 00 3a 00 31 00 32 00 3a 00 32 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-02-06T22:12:27Z">	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7680	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7684	2	09 00		success or wait	2	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7688	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 37 00 31 00 36 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 30 00 36 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 36 00 32 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="306" PID="5716" UptimeMS="1062" TimeSinceCreationMS="1062" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7950	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7954	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7958	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7978	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7982	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	7984	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	8022	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	8026	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	8028	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	8066	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	8070	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	8074	98	3c 00 47 00 75 00 69 00 64 00 3e 00 34 00 61 00 62 00 36 00 30 00 34 00 65 00 30 00 2d 00 66 00 65 00 39 00 39 00 2d 00 34 00 30 00 37 00 38 00 2d 00 38 00 33 00 62 00 31 00 2d 00 37 00 33 00 38 00 36 00 37 00 34 00 33 00 38 00 32 00 39 00 32 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>4ab604e0-fe99-4078-83b1-73867438292b</Guid>	success or wait	1	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	8172	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	8176	2	09 00		success or wait	2	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	8180	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 36 00 54 00 32 00 32 00 3a 00 31 00 32 00 3a 00 32 00 37 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>2023-02-06T22:12:27Z</CreationTime>	success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	8278	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	8282	2	09 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	8284	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	8324	4	0d 00 0a 00		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER756B.tmp.WERInternalMetadata.xml	8328	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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER75D9.tmp.xml	0	4678	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 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 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 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	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_tpyienirbwgp.exe_491668454d7886d02c78a9f3324eec6e9b560bc_bb377917_156a7e34\Report.wer	0	2	fd fd		success or wait	1	68DA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_tpyienirbwgp.exe_491668454d7886d02c78a9f3324eec6e9b560bc_bb377917_156a7e34\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	172	68DA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_tpyienirbwgp.exe_491668454d7886d02c78a9f3324eec6e9b560bc_bb377917_156a7e34\Report.wer	11756	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 2d 00 39 00 30 00 38 00 32 00 34 00 38 00 31 00 32 00 38 00	MetadataHash=-908248128	success or wait	1	68DA497A	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

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

Analysis Process: tpyienirbwgp.exe PID: **5408**, Parent PID: **3324**

General

Target ID:	7
Start time:	14:12:30
Start date:	06/02/2023
Path:	C:\Users\user\AppData\Roaming\swschqavfbk\tpyienirbwgp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\swschqavfbk\tpyienirbwgp.exe" "C:\Users\user\AppData\Local\Temp\tohjyweui.exe" C:\Users\user\A
Imagebase:	0x990000
File size:	370176 bytes
MD5 hash:	64517EEC55E1F3C392B63B73D833E5F9
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: **4032**, Parent PID: **5408**

General

Target ID:	9
Start time:	14:12:31
Start date:	06/02/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5408 -s 604
Imagebase:	0x890000
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

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	68E61717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84EC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84EC.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	68E5497A	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_tpyienirbwgp.exe_491668454d7886d02c78a9f3324eec6e9b560bc_bb377917_0f868df3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_tpyienirbwgp.exe_491668454d7886d02c78a9f3324eec6e9b560bc_bb377917_0f868df3\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	68E5497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84EC.tmp	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84EC.tmp.xml	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER850C.tmp.csv	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8607.tmp.txt	success or wait	1	68E5497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 4f 7b fd 63 fd 05 12 00 00 00 00 00	MDMP O{c	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	7396	6	00 00 00 00 00 00		success or wait	1	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.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 20 15 00 00 4e 7b 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	UBGenuineIntelWT N{c Pacific Standard TimePacific Daylight T ime	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	8660	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 30 fd 0f 01 00 00 00 00 30 fd 6d 76 fd 01 00 00 05 00 00 00 01 00 00 00 fd fd 0f 01 fd 1b 00 23 00 00 00 02 02 00 00 fd fd 0f 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++00mv#+	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	1620	168	fd 14 00 00 00 00 00 00 09 04 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 fd 1b 00 00 00 00 00 01 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	!	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	12240	20	11 00 00 00 3c fd 0f 77 00 00 00 00 00 00 01 00 00 fd 30 00 00	<w0	success or wait	17	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	12516	256	fd 10 00 fd fd fd 01 00 00 fd fd fd 10 77 fd fd fd 0c 00 fd fd fd 01 00 00 fd fd fd 10 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 10 77 fd fd fd 1c 00 fd fd fd 01 00 00 fd fd fd 10 77 fd fd fd 08 00 fd fd fd 01 06 00 fd fd fd 10 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd fd 10 77 fd fd fd 10 00 fd fd fd 01 15 00 fd fd fd 10 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd fd 10 77 fd fd fd 14 00 fd fd fd 01 03 00 fd fd fd 10 77 fd fd fd 04 00 fd fd fd 01 03 00 fd fd fd 10 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 10 77 fd fd fd 14 00 fd fd fd 01 00 00 fd fd fd 10 77 fd fd cd 49 00 fd fd 01 00 00 fd fd fd 10 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd fd 10 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd fd 10 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 10 77 fd	wwwwwwwwwwwwlwwww	success or wait	16	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	34376	1064	fd fd 0f 77 fd fd 0d 77 fd 00 00 00 fd fd fd fd 10 00 00 00 6c fd 55 01 38 fd 55 01 fd fd fd fd 40 fd 0d 77 40 fd 0d 77 fd fd fd fd 00 fd fd 00 00 fd fd 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 08 31 19 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd 19 01 00 00 00 00 00 00 00 00 00 33 19 01 00 10 fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd 18 fd 65 01 2c fd 45 01 20 fd 65 01 34 fd 45 01 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwlU8U@w@w13e,Ee4E	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	1788	4	04 00 00 00		success or wait	4	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	9376	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 30 fd 0f 01 00 00 00 00 30 fd 6d 76 fd 01 00 00 fd fd fd fd fd fd fd fd fd 0f 01 fd 1b 00 23 00 00 00 02 02 00 00 fd fd 0f 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++00mv#+	success or wait	4	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	1936	48	04 12 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 4c fd 65 01 00 00 00 00 fd 03 00 00 1c 7a 00 00 fd 02 00 00 04 2d 00 00	Lez-	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	1996	4	2c 00 00 00	,	success or wait	44	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	7402	38	20 00 00 00 74 00 70 00 79 00 69 00 65 00 6e 00 69 00 72 00 62 00 77 00 67 00 70 00 2e 00 65 00 78 00 65 00 00 00	tpyienirbwgp.exe	success or wait	44	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	6644	752	00 00 3a 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 fd fd 02 00 00 00 00 00 fd 46 03 00 00 00 00 1b fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 53 fd 03 00 00 00 00 00 19 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 15 67 06 00 00 00 00	:s*,!BB?%@AZbFS@g	success or wait	1	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.tmp.dmp	35440	8716	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 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82C8.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 14 01 00 00 fd 2f 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 17 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 60 1a 00 00 16 00 00 00 fd 00 00 00 4c 1c 00 00	/T8T`L	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.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	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 34 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5408</Pid>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1002	78	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 74 00 70 00 79 00 69 00 65 00 6e 00 69 00 72 00 62 00 77 00 67 00 70 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>tpyienirbwgp.exe</ImageName>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1080	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1084	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1088	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1178	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1182	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1186	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 37 00 39 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1799</Uptime>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1228	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1232	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1236	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1318	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1322	2	09 00		success or wait	2	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1326	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1378	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1382	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1386	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1430	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1434	2	09 00		success or wait	3	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1440	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 34 00 33 00 39 00 36 00 34 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>94396416</PeakVirtualSize>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1536	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 33 00 37 00 39 00 30 00 32 00 30 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>93790208</VirtualSize>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1606	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1610	2	09 00		success or wait	3	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1616	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 32 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>2025</PageFaultCount>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1690	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1694	2	09 00		success or wait	3	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1700	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 32 00 31 00 36 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7921664</PeakWorkingSetSize>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1796	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1800	2	09 00		success or wait	3	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1806	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 32 00 31 00 36 00 36 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7921664</WorkingSetSize>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1886	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1890	2	09 00		success or wait	3	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	1896	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 38 00 37 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>178728</QuotaPeakPagedPoolUsage>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2010	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2014	2	09 00		success or wait	3	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2020	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 37 00 35 00 34 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>177544</QuotaPagedPoolUsage>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2118	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2122	2	09 00		success or wait	3	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2128	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 35 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>22528</QuotaPeakNonPagedPoolUsage>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2252	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2256	2	09 00		success or wait	3	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2262	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 33 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>22392</QuotaNonPagedPoolUsage>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2370	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2374	2	09 00		success or wait	3	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2380	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 36 00 31 00 32 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1761280</PagefileUsage>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2456	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2460	2	09 00		success or wait	3	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2466	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 36 00 35 00 33 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1765376</PeakPagefileUsage>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2558	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2562	2	09 00		success or wait	3	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2568	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 36 00 31 00 32 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1761280</PrivateUsage>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2640	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2644	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2648	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2694	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2698	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2702	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2732	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2736	2	09 00		success or wait	3	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2742	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2782	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2786	2	09 00		success or wait	4	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2794	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2824	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2828	2	09 00		success or wait	4	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2836	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2906	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2910	2	09 00		success or wait	4	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	2918	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3008	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3012	2	09 00		success or wait	4	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3020	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 36 00 32 00 30 00 36 00 30 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4620601</Uptime>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3068	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3072	2	09 00		success or wait	4	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3080	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3158	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3162	2	09 00		success or wait	4	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3170	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3222	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3226	2	09 00		success or wait	4	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3234	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3278	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3282	2	09 00		success or wait	5	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3292	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3382	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3386	2	09 00		success or wait	5	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3396	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3470	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3474	2	09 00		success or wait	5	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3484	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 38 00 34 00 34 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>68446</PageFaultCount>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3560	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3564	2	09 00		success or wait	5	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3574	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 36 00 38 00 35 00 33 00 31 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>126853120</PeakWorkingSetSize>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3674	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3678	2	09 00		success or wait	5	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3688	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 35 00 37 00 39 00 32 00 32 00 35 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>125792256</WorkingSetSize>	success or wait	1	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3772	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3776	2	09 00		success or wait	5	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3786	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 38 00 30 00 35 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11805 12</QuotaPeakPagedPoolUsage>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3902	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3906	2	09 00		success or wait	5	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	3916	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 31 00 33 00 32 00 38 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1132856</ QuotaPagedPoolUsage>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4016	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4020	2	09 00		success or wait	5	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4030	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 31 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>91 984</QuotaPeakNonPagedPoolUsage>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4154	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4158	2	09 00		success or wait	5	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4168	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 33 00 30 00 36 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>83064< /QuotaNonPagedPoolUsage>	success or wait	1	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4276	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4280	2	09 00		success or wait	5	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4290	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 36 00 35 00 31 00 34 00 31 00 37 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>46514176</PagefileUsage>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4368	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4372	2	09 00		success or wait	5	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4382	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 35 00 34 00 32 00 32 00 37 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>47542272</PeakPagefileUsage>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4476	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4480	2	09 00		success or wait	5	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4490	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 36 00 35 00 31 00 34 00 31 00 37 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>46514176</PrivateUsage>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4564	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4568	2	09 00		success or wait	4	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4576	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	3	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4632	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4674	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4678	2	09 00		success or wait	2	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4682	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4720	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4762	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4766	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4768	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4806	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4810	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4814	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	9	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	18	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	4874	82	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 74 00 70 00 79 00 69 00 65 00 6e 00 69 00 72 00 62 00 77 00 67 00 70 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>tpyienirbwgp.exe</Parameter0>	success or wait	9	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	5560	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	5564	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	5566	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	5606	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	5610	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	5612	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	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	5650	4	0d 00 0a 00		success or wait	6	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	5654	2	09 00		success or wait	12	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	5658	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6212	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6216	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6218	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6258	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6262	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6264	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6302	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6306	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6310	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6404	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6408	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6412	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 6c 00 67 00 6a 00 70 00 72 00 6b 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>lgjprk, Inc.</SystemManufacturer>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6518	4	0d 00 0a 00		success or wait	1	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6522	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6526	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 6c 00 67 00 6a 00 70 00 72 00 6b 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>lgjprk7,1</SystemProductName>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6622	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6626	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6630	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6750	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6754	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6758	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 33 00 35 00 38 00 34 00 30 00 32 00 35 00 32 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>1635840252</OSInstallDate>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6840	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6844	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6848	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6950	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6954	2	09 00		success or wait	2	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	6958	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7026	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7030	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7032	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7072	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7076	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7078	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7112	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7116	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7120	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7216	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7220	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7222	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7258	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7262	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7264	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7288	4	0d 00 0a 00		success or wait	3	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7292	2	09 00		success or wait	6	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7296	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 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>80000000</Flags>	success or wait	3	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7540	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7544	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7546	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7572	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7576	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7578	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 36 00 54 00 32 00 32 00 3a 00 31 00 32 00 3a 00 33 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-02-06T22:12:31Z">	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7678	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7682	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7686	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 31 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 34 00 30 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 39 00 30 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 39 00 30 00 36 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="311" PID="5408" UptimeMS="906" TimeSinceCreationMS="906" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7952	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	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7972	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7976	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	7978	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	8016	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	8020	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	8022	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	8060	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	8064	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	8068	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 62 00 63 00 66 00 63 00 38 00 31 00 33 00 2d 00 31 00 62 00 36 00 31 00 2d 00 34 00 33 00 66 00 37 00 2d 00 39 00 61 00 64 00 36 00 2d 00 63 00 30 00 65 00 62 00 61 00 33 00 36 00 32 00 38 00 61 00 36 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>6bcfc813-1b61-43f7-9ad6-c0eba3628a6e</Guid>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	8166	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	8170	2	09 00		success or wait	2	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	8174	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 36 00 54 00 32 00 32 00 3a 00 31 00 32 00 3a 00 33 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-02-06T22:12:31Z</CreationTime>	success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	8272	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	8276	2	09 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	8278	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	8318	4	0d 00 0a 00		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84BD.tmp.WERInternalMetadata.xml	8322	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	68E5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER84EC.tmp.xml	0	4678	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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_tpyienirbwgp.exe_491668454d7886d02c78a9f3324eec6e9b560bc_bb377917_0f868df3\Report.wer	0	2	fd fd		success or wait	1	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_tpyienirbwgp.exe_491668454d7886d02c78a9f3324eec6e9b560bc_bb377917_0f868df3\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	68E5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_tpyienirbwgp.exe_491668454d7886d02c78a9f3324eec6e9b560bc_bb377917_0f868df3\Report.wer	11656	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 33 00 39 00 32 00 35 00 36 00 31 00 35 00 37 00 30 00	MetadataHash=392561570	success or wait	1	68E5497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly