ID: 1439879
Sample Name: upfilles.dll.exe
Cookbook: default.jbs
Time: 00:03:08
Date: 11/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

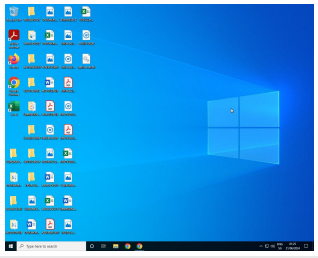
Windows Analysis Report

upfilles.dll.dll

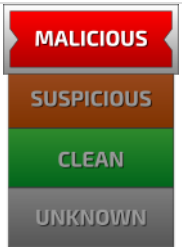
Overview

General Information

Sample name:	upfilles.dll.dll (renamed file extension from exe to dll)
Original sample name:	upfilles.dll.exe
Analysis ID:	1439879
MD5:	ccb6d3cb020f5..
SHA1:	4a013f752c2bf…
SHA256:	f4cb6b684ea09..
Tags:	exe
Infos:	



Detection



Bazar Loader, BruteRatel, Latrodectus

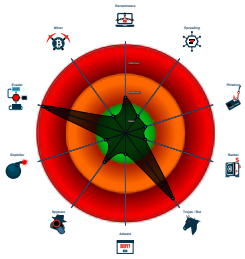
Score: 100

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected Bazar Loader
- Yara detected BruteRatel
- Yara detected Latrodectus
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Contains functionality to inject threa…
- Creates a thread in another existing…
- Injects a PE file into a foreign proce…
- Injects code into the Windows Explo…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6632 cmdline: loaddll64.exe "C:\Users\user\Desktop\upfilles.dll.dll" MD5: 763455F9DCB24DFEECC2B9D9F8D46D52)
  - conhost.exe (PID: 6636 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - cmd.exe (PID: 344 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\upfilles.dll.dll",#1 MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
    - rundll32.exe (PID: 5472 cmdline: rundll32.exe "C:\Users\user\Desktop\upfilles.dll.dll",#1 MD5: EF3179D498793BF4234F708D3BE28633)
  - regsvr32.exe (PID: 2180 cmdline: regsvr32.exe /i /s C:\Users\user\Desktop\upfilles.dll.dll MD5: B0C2FA35D14A9FAD919E99D9D75E1B9E)
  - rundll32.exe (PID: 6296 cmdline: rundll32.exe C:\Users\user\Desktop\upfilles.dll.dll,DllCanUnloadNow MD5: EF3179D498793BF4234F708D3BE28633)
  - rundll32.exe (PID: 6324 cmdline: rundll32.exe C:\Users\user\Desktop\upfilles.dll.dll,DllGetClassObject MD5: EF3179D498793BF4234F708D3BE28633)
    - WerFault.exe (PID: 6688 cmdline: C:\Windows\system32\WerFault.exe -u -p 6324 -s 344 MD5: FD27D9F6D02763BDE32511B5DF7FF7A0)
  - rundll32.exe (PID: 6516 cmdline: rundll32.exe C:\Users\user\Desktop\upfilles.dll.dll,DllInstall MD5: EF3179D498793BF4234F708D3BE28633)
    - WerFault.exe (PID: 3732 cmdline: C:\Windows\system32\WerFault.exe -u -p 6516 -s 344 MD5: FD27D9F6D02763BDE32511B5DF7FF7A0)
  - rundll32.exe (PID: 7264 cmdline: rundll32.exe "C:\Users\user\Desktop\upfilles.dll.dll",DllCanUnloadNow MD5: EF3179D498793BF4234F708D3BE28633)
  - rundll32.exe (PID: 7272 cmdline: rundll32.exe "C:\Users\user\Desktop\upfilles.dll.dll",DllGetClassObject MD5: EF3179D498793BF4234F708D3BE28633)
    - WerFault.exe (PID: 7388 cmdline: C:\Windows\system32\WerFault.exe -u -p 7272 -s 344 MD5: FD27D9F6D02763BDE32511B5DF7FF7A0)
  - rundll32.exe (PID: 7288 cmdline: rundll32.exe "C:\Users\user\Desktop\upfilles.dll.dll",DllInstall MD5: EF3179D498793BF4234F708D3BE28633)
    - WerFault.exe (PID: 7396 cmdline: C:\Windows\system32\WerFault.exe -u -p 7288 -s 344 MD5: FD27D9F6D02763BDE32511B5DF7FF7A0)
  - rundll32.exe (PID: 7296 cmdline: rundll32.exe "C:\Users\user\Desktop\upfilles.dll.dll",DllUnregisterServer MD5: EF3179D498793BF4234F708D3BE28633)
  - rundll32.exe (PID: 7320 cmdline: rundll32.exe "C:\Users\user\Desktop\upfilles.dll.dll",stow MD5: EF3179D498793BF4234F708D3BE28633)
    - explorer.exe (PID: 2580 cmdline: C:\Windows\Explorer.EXE MD5: 662F4F92FDE3557E86D110526BB578D5)
      - rundll32.exe (PID: 7856 cmdline: "C:\Windows\system32\rundll32.exe" "C:\Users\user\AppData\Roaming\upfilles.dll", stow MD5: EF3179D498793BF4234F708D3BE28633)
      - rundll32.exe (PID: 7984 cmdline: "C:\Windows\system32\rundll32.exe" "C:\Users\user\AppData\Roaming\upfilles.dll", stow MD5: EF3179D498793BF4234F708D3BE28633)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Brute Ratel C4, BruteRatel	Brute Ratel is a a Customized Command and Control Center for Red Team and Adversary SimulationSMB and TCP payloads provide functionality to write custom external C2 channels over legitimate websites such as Slack, Discord, Microsoft Teams and more.Built-in debugger to detect EDR userland hooks.Ability to keep memory artifacts hidden from EDRs and AV.Direct Windows SYS calls on the fly.	No Attribution	http://https://0xdarkvortex.dev/hiding-in-plainsight/https://0xdarkvortex.dev/proxying-dll-loads-for-hiding-etwti-stack-tracing/https://andreafortuna.org/2023/02/23/how-to-detect-brute-ratel-activitieshttps://blog.spookysec.net/analyzing-brc4-badgers/https://bruteratel.com/research/feature-update/2021/06/01/PE-Reflection-Long-Live-The-King/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.brute_ratel_c4

Name	Description	Attribution	Blogpost URLs	Link
Unidentified 111 (Latrodectus), Latrodectus	First discovered in October 2023, BLACKWIDOW is a backdoor written in C that communicates over HTTP using RC4 encrypted requests. The malware has the capability to execute discovery commands, query information about the victim's machine, update itself, as well as download and execute an EXE, DLL, or shellcode. The malware is believed to have been developed by LUNAR SPIDER, the creators of IcedID (aka BokBot) Malware.	No Attribution	http://https://0x0d4y.blog/latrodectus-technical-analysis-of-the-new-icedid/https://embee-research.ghost.io/phishing-domain-analysis-with-passive-dns-latrodectus/https://exchange.xforce.ibmcloud.com/malware-analysis/guid:dab8a02f9161933bc2eff5ba4a5f8412https://github.com/VenzoV/MalwareAnalysisReports/blob/main/Latrodectus/Latrodectus%20%22Littlehw%22.mdhttps://medium.com/walmartglobaltech/icedid-gets-loaded-af073b7b6d39	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_111

Malware Configuration

Threatname: Latrodectus


```
{
  "C2 url": [
    "https://workspacin.cloud/live/",
    "https://illoskanawer.com/live/"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000003.2703639060.0000000003250000.00000040.00000001.00020000.00000000.sdmp	JoeSecurity_Latrodectus	Yara detected Latrodectus	Joe Security	
00000012.00000003.2415718994.000002921161C000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_BruteRatel_1	Yara detected BruteRatel	Joe Security	
00000012.00000003.1868997096.000002921161C000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_BruteRatel_1	Yara detected BruteRatel	Joe Security	
00000012.00000003.2680109233.000002921161C000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_BruteRatel_1	Yara detected BruteRatel	Joe Security	
00000012.00000003.1843049394.0000029213423000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_BruteRatel_1	Yara detected BruteRatel	Joe Security	
Click to see the 35 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
18.3.rundll32.exe.7df4f0220000.0.unpack	JoeSecurity_Latrodectus	Yara detected Latrodectus	Joe Security	

Source	Rule	Description	Author	Strings
22.0.explorer.exe.13a0000.0.unpack	JoeSecurity_Latrodectus	Yara detected Latrodectus	Joe Security	
18.3.rundll32.exe.7df4f0220000.0.raw.unpack	JoeSecurity_Latrodectus	Yara detected Latrodectus	Joe Security	
22.0.explorer.exe.13a0000.0.raw.unpack	JoeSecurity_Latrodectus	Yara detected Latrodectus	Joe Security	
22.2.explorer.exe.13a0000.0.unpack	JoeSecurity_Latrodectus	Yara detected Latrodectus	Joe Security	
Click to see the 4 entries				

Sigma Signatures

System Summary

Sigma detected: RunDLL32 Spawning Explorer

Sigma detected: CurrentVersion Autorun Keys Modification

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Sample uses string decryption to hide its real strings

Networking

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

C2 URLs / IPs found in malware configuration

HIPS / PFW / Operating System Protection Evasion

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

Allocates memory in foreign processes

Contains functionality to inject threads in other processes

Creates a thread in another existing process (thread injection)

Injects a PE file into a foreign processes

Injects code into the Windows Explorer (explorer.exe)

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

Sets debug register (to hijack the execution of another thread)

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected Bazar Loader

Yara detected BruteRatel

Yara detected Latrodectus

Remote Access Functionality

Yara detected Bazar Loader

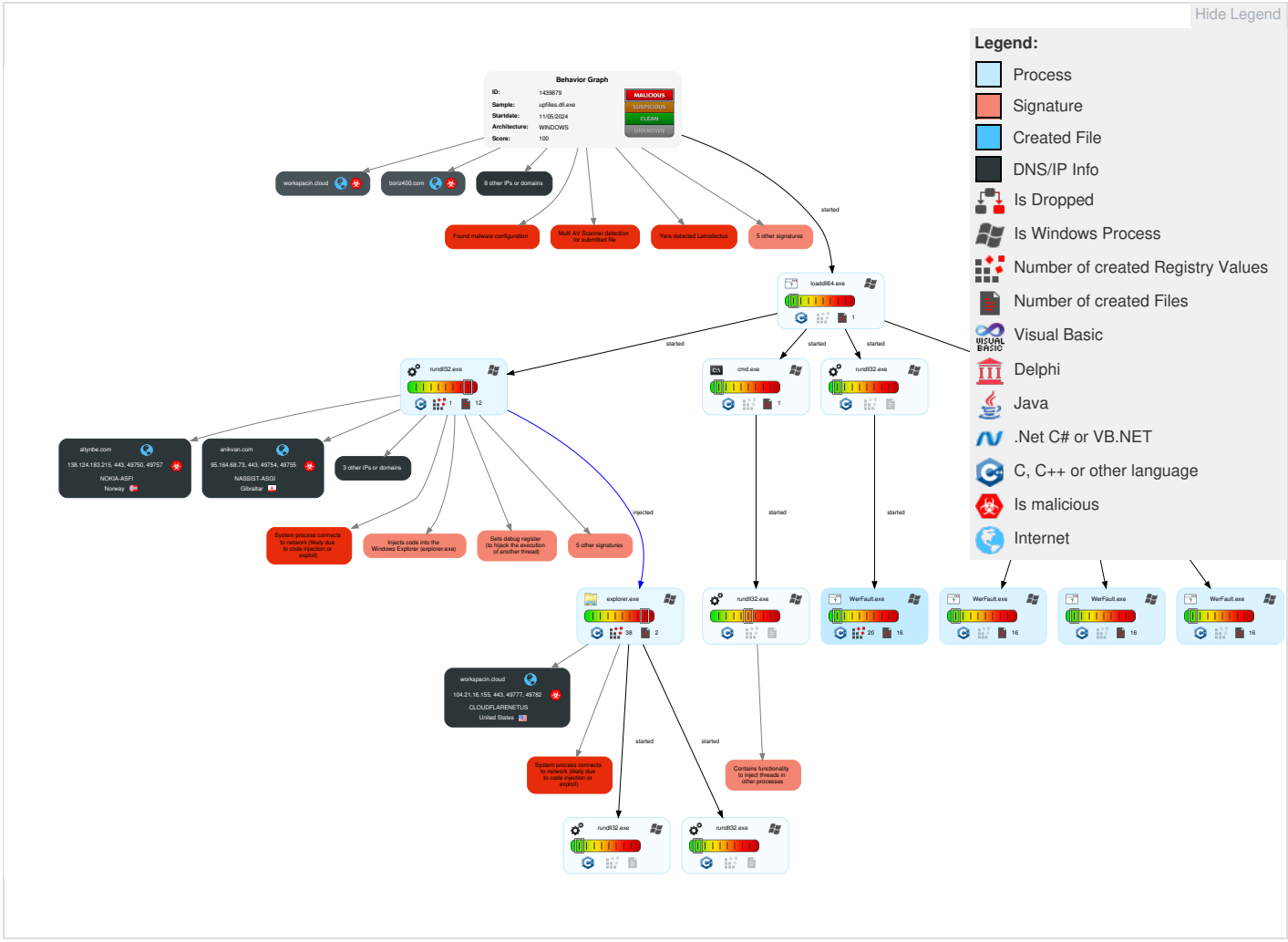
Yara detected BruteRatel

Yara detected Latrodectus

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	9 1 2 Process Injection	2 1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	1 1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 Registry Run Keys / Startup Folder	9 1 2 Process Injection	LSASS Memory	5 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	3 Ingress Tool Transfer	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	1 DLL Side-Loading	1 Obfuscated Files or Information	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	3 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 Regsvr32	NTDS	3 Process Discovery	Distributed Component Object Model	Input Capture	1 1 4 Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Rundll32	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 DLL Side-Loading	Cached Domain Credentials	1 Account Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	Compile After Delivery	DCSync	1 System Owner/User Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 System Network Configuration Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	HTML Smuggling	/etc/passwd and /etc/shadow	2 File and Directory Discovery	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement
IP Addresses	Compromise Infrastructure	Supply Chain Compromise	PowerShell	Cron	Cron	Dynamic API Resolution	Network Sniffing	1 3 System Information Discovery	Shared Webroot	Local Data Staging	File Transfer Protocols	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	External Defacement

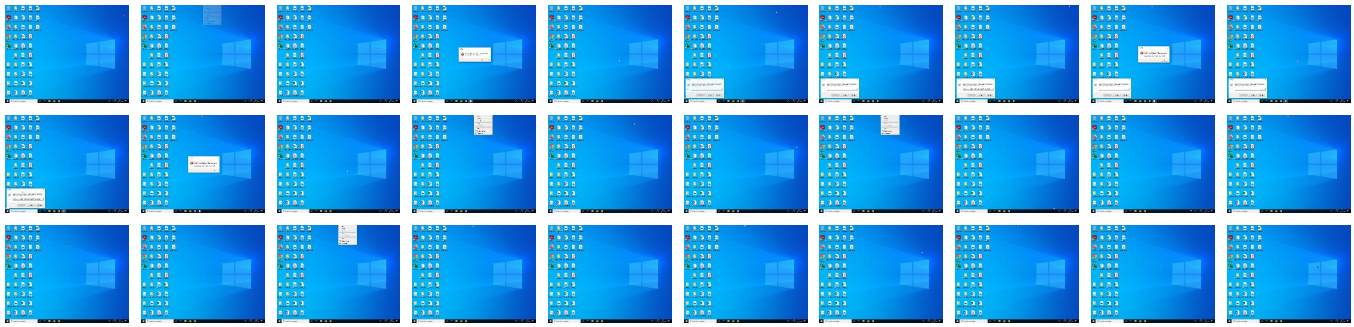
Behavior Graph



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
upfilles.dll.dll	16%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://simpleflying.com/how-do-you-become-an-air-traffic-controller/	0%	URL Reputation	safe	
http://https://img.s-msn.com/tenant/amp/entityid/AAbC0oi.img	0%	URL Reputation	safe	
http://https://outlook.com_	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azure(	0%	Avira URL Cloud	safe	
http://https://altynbe.com/tyk.io	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azure	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azure4	0%	Avira URL Cloud	safe	
http://https://anikvan.com/content.php	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/	0%	Avira URL Cloud	safe	
http://https://boriz400.com/api/azurey	0%	Avira URL Cloud	safe	
http://https://illoskanawer.com/live/	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azure=	0%	Avira URL Cloud	safe	
http://https://powerpoint.office.comcember	0%	URL Reputation	safe	
http://https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/api/azure	0%	Avira URL Cloud	safe	
http://schemas.micro	0%	URL Reputation	safe	
http://https://altynbe.com/content.php	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/content.phpP	0%	Avira URL Cloud	safe	
http://https://anikvan.com/l~	0%	Avira URL Cloud	safe	
http://https://anikvan.com/	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/f	0%	Avira URL Cloud	safe	
http://https://boriz400.com/api/azure	0%	Avira URL Cloud	safe	
http://https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/content.php4	0%	Avira URL Cloud	safe	
http://https://anikvan.com/content.php.f	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/content.php1j	0%	Avira URL Cloud	safe	
http://https://workspacin.cloud/live/0vaH	0%	Avira URL Cloud	safe	
http://https://altynbe.com/U~	0%	Avira URL Cloud	safe	
http://https://workspacin.cloud/live/6	0%	Avira URL Cloud	safe	
http://https://altynbe.com/B_F	0%	Avira URL Cloud	safe	
http://https://anikvan.com/content.phpGf	0%	Avira URL Cloud	safe	
http://https://altynbe.com/content.php2f	0%	Avira URL Cloud	safe	
http://https://anikvan.com/api/azuret.php.f	0%	Avira URL Cloud	safe	
http://https://altynbe.com/	0%	Avira URL Cloud	safe	
http://https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/content.phpL	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azurent.php	0%	Avira URL Cloud	safe	
http://https://anikvan.com/d	0%	Avira URL Cloud	safe	
http://https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/content.php	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azurep1j	0%	Avira URL Cloud	safe	
http://https://altynbe.com/api/azureontent.phpMfE	0%	Avira URL Cloud	safe	
http://https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/content.phpA	0%	Avira URL Cloud	safe	
http://https://altynbe.com/api/azure	0%	Avira URL Cloud	safe	
http://https://workspacin.cloud/live/J5	0%	Avira URL Cloud	safe	
http://https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/content.phpLgF	0%	Avira URL Cloud	safe	
http://https://boriz400.com/qa	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azure.php	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/content.php&j	0%	Avira URL Cloud	safe	
http://https://workspacin.cloud/	0%	Avira URL Cloud	safe	
http://https://boriz400.com/content.php	0%	Avira URL Cloud	safe	
http://https://altynbe.com/X	0%	Avira URL Cloud	safe	
http://https://altynbe.com/d	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azurepP	0%	Avira URL Cloud	safe	
http://https://anikvan.com/api/azure==	0%	Avira URL Cloud	safe	
http://https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/content.phpMfE	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azurepjB	0%	Avira URL Cloud	safe	
http://https://boriz400.com/	0%	Avira URL Cloud	safe	
http://https://altynbe.com/5~	0%	Avira URL Cloud	safe	
http://https://altynbe.com/api/azureure	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/content.php4	0%	Avira URL Cloud	safe	
http://https://altynbe.com/=~	0%	Avira URL Cloud	safe	
http://https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/n	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/content.php	0%	Avira URL Cloud	safe	
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azurep&j	0%	Avira URL Cloud	safe	
http://https://workspacin.cloud/live/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://anikvan.com/api/azure	0%	Avira URL Cloud	safe	
http://https://altynbe.com/api/azurep	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
workspacin.cloud	104.21.16.155	true	true		unknown
ae1f8849daaac4ee6b80681872ab88b9-1762121307.eu-central-1.elb.amazonaws.com	3.69.236.35	true	false		high
boriz400.com	91.194.11.183	true	true		unknown
altynbe.com	138.124.183.215	true	true		unknown
anikvan.com	95.164.68.73	true	true		unknown
ae97372e4f96e4d1299fbaeb7130b656-1584023256.us-east-1.elb.amazonaws.com	54.175.181.104	true	false		high
uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io	unknown	unknown	false		unknown
ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://illoskanawer.com/live/	true	• Avira URL Cloud: safe	unknown
https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azure	true	• Avira URL Cloud: safe	unknown
https://anikvan.com/content.php	true	• Avira URL Cloud: safe	unknown
https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/api/azure	true	• Avira URL Cloud: safe	unknown
https://altynbe.com/content.php	true	• Avira URL Cloud: safe	unknown
https://boriz400.com/api/azure	true	• Avira URL Cloud: safe	unknown
https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/content.php	true	• Avira URL Cloud: safe	unknown
https://altynbe.com/api/azure	true	• Avira URL Cloud: safe	unknown
https://boriz400.com/content.php	true	• Avira URL Cloud: safe	unknown
https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/content.php	true	• Avira URL Cloud: safe	unknown
https://workspacin.cloud/live/	true	• Avira URL Cloud: safe	unknown
https://anikvan.com/api/azure	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/odirmr	explorer.exe, 00000016.00000000.1846357884.00000000079FB000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000002.2940539964.00000000079FB000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azure4	rundll32.exe, 00000012.00000003.2680109233.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2762031046.000002921163E000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2797600040.000002921163E000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2738453835.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2491436893.000002921163E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.query.prod.cms.msn.com/cms/api/amp/binary/AA13f2DV	explorer.exe, 00000016.00000002.2940539964.0000000007900000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.1846357884.0000000007900000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azure=	rundll32.exe, 00000012.00000003.2415718994.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2680109233.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2810618243.000002921163E000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000002.2938154508.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2311970800.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2397236802.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2762031046.000002921163E000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2797600040.000002921163E000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2738453835.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2284307888.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2042061481.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2491436893.000002921163E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://altynbe.com/tyk.io	rundll32.exe, 00000012.00000003.2001079033.000002921161C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/	rundll32.exe, 00000012.00000003.2797091473.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2042061481.00000292115EF000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2311970800.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2397236802.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2810418995.00000292115EF000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2738453835.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2284307888.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2042061481.000002921161C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.msn.com:443/v1/news/Feed/Windows?	explorer.exe, 00000016.00000000.1847916203.00000000097D4000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000002.2940539964.000000000790000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.1846357884.000000007900000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000002.2942821965.00000000097D4000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://boriz400.com/api/azurey	rundll32.exe, 00000012.00000003.2762031046.00000292115AE000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2810418995.00000292115AE000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2738453835.00002921158B000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.1882651450.00000292115BC000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2680109233.00000292115BB000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2415718994.00000292115AE000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2284190577.00000292115AE000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2311847302.00000292115AE000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2797091473.00000292115AE000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000002.2938154508.00000292115AE000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2397236802.0000029 2115AE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azure(	rundll32.exe, 00000012.00000002.2938154508.00000292115EF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://excel.office.com	explorer.exe, 00000016.00000002.2945734291.000000000C5AA000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.1859052974.000000000C5AA000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.msn.com/en-us/news/us/a-nationwide-emergency-alert-will-be-sent-to-all-u-s-cellphones-we	explorer.exe, 00000016.00000002.2940539964.0000000007900000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.1846357884.0000000007900000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://simpleflying.com/how-do-you-become-an-air-traffic-controller/	explorer.exe, 00000016.00000002.2940539964.0000000007900000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.1846357884.0000000007900000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/content.phpP	rundll32.exe, 00000012.00000003.2680109233.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2311970800.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2762031046.000002921163E000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2797600040.000002921163E000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2738453835.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2491436893.000002921163E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://anikvan.com/l~	rundll32.exe, 00000012.00000002.2938154508.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2762031046.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2797091473.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2810418995.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2738453835.000002921161C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.query.prod.cms.msn.com/cms/api/amp/binary/AA13gTUY	explorer.exe, 00000016.00000002.2940539964.0000000007900000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.1846357884.0000000007900000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://cdn.query.prod.cms.msn.com/cms/api/amp/binary/AA13gHZu-dark	explorer.exe, 00000016.00000000.1846357884.00000000078AD000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000002.2940539964.00000000078AD000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/f	rundll32.exe, 00000012.00000003.27970914 73.000002921161C000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0012.00000003.2810418995.000002921161C00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://activity.windows.com/UserActivity.ReadWrite.CreatedByAppcrobat.exe	explorer.exe, 00000016.00000002.29457342 91.000000000C893000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1859052974.000000000C89300 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://anikvan.com/	rundll32.exe, 00000012.00000003.22841905 77.00000292115AE000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0012.00000003.2311970800.000002921161C00 0.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2397236802.000 002921161C000.00000004.00000020.00020000 .00000000.sdmp, rundll32.exe, 00000012.0 0000003.2001079033.000002921161C000.0000 0004.00000020.00020000.00000000.sdmp, ru ndll32.exe, 00000012.00000003.2810418995 .000002921161C000.00000004.00000020.0002 0000.00000000.sdmp, rundll32.exe, 000000 12.00000003.2738453835.000002921161C000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2284307888.00000 2921161C000.00000004.00000020.00020000.0 0000000.sdmp, rundll32.exe, 00000012.000 00003.1882552320.000002921161C000.000000 04.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2042061481.00000292116 1C000.00000004.00000020.00020000.0000000 0.sdmp, rundll32.exe, 00000012.00000003. 1991839967.000002921161C000.00000004.000 00020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/content.php1j	rundll32.exe, 00000012.00000003.23119708 00.000002921161C000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://assets.msn.com/weathermapdata/1/static/weather/Icons/JyNGQgA=/Condition/AAehR3S.svg	explorer.exe, 00000016.00000000.18463578 84.0000000007900000.00000004.00000001.00 020000.00000000.sdmp	false		high
http://https://anikvan.com/content.php.f	rundll32.exe, 00000012.00000003.22843078 88.000002921161C000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000016.00000000.18590529 74.000000000C964000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000002.2945734291.000000000C96400 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://wns.windows.com/L	explorer.exe, 00000016.00000000.18590529 74.000000000C557000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000002.2945734291.000000000C55700 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/content.php4	rundll32.exe, 00000012.00000003.22841905 77.000002921159F000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0012.00000003.2762031046.000002921159F00 0.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2311847302.000 002921159F000.00000004.00000020.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://word.office.com	explorer.exe, 00000016.00000002.29457342 91.000000000C5AA000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1859052974.000000000C5AA00 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://workspacin.cloud/live/0vaH	explorer.exe, 00000016.00000002.29435545 99.00000000098A8000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://altynbe.com/U~	rundll32.exe, 00000012.00000003.18689970 96.000002921161C000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0012.00000003.2415718994.000002921161C00 0.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2680109233.000 002921161C000.00000004.00000020.00020000 .00000000.sdmp, rundll32.exe, 00000012.0 0000002.2938154508.000002921161C000.0000 0004.00000020.00020000.00000000.sdmp, ru ndll32.exe, 00000012.00000003.2762031046 .000002921161C000.00000004.00000020.0002 0000.00000000.sdmp, rundll32.exe, 000000 12.00000003.2797091473.000002921161C000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2311970800.00000 2921161C000.00000004.00000020.00020000.0 0000000.sdmp, rundll32.exe, 00000012.000 00003.2397236802.000002921161C000.000000 04.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2001079033.00000292116 1C000.00000004.00000020.00020000.0000000 0.sdmp, rundll32.exe, 00000012.00000003. 2810418995.000002921161C000.00000004.000 00020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2738453835.0000029 21161C000.00000004.00000020.00020000.000 00000.sdmp, rundll32.exe, 00000012.00000 003.2284307888.000002921161C000.00000004 .00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.1842659886.000002921161C 000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.1882552320.0 00002921161C000.00000004.00000020.000200 00.00000000.sdmp, rundll32.exe, 00000012 .00000003.2042061481.000002921161C000.00 000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.19918399 67.000002921161C000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0012.00000003.1867444760.000002921161C00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://altynbe.com/B_F	rundll32.exe, 00000012.00000003.26801092 33.00000292115BB000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://assets.msn.com/weathermapdata/1/static/financ e/1stparty/FinanceTaskbarIcons/Finance_Earnings	explorer.exe, 00000016.00000000.18463578 84.0000000007900000.00000004.00000001.00 020000.00000000.sdmp	false		high
http:// https://cdn.query.prod.cms.msn.com/cms/api/amp/bina ry/AA13gHZu	explorer.exe, 00000016.00000000.18463578 84.00000000078AD000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000002.2940539964.00000000078AD00 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://workspacin.cloud/live/6	explorer.exe, 00000016.00000002.29470273 90.000000000CA7C000.00000004.00000001.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://uncertain-kitten-gw.aws-euc1.cloud- ara.tyk.io/F	rundll32.exe, 00000012.00000002.29381545 08.000002921161C000.00000004.00000020.00 020000.00000000.sdmp	false		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://anikvan.com/content.phpGf	rundll32.exe, 00000012.00000003.2415718994.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2680109233.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000002.2938154508.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2762031046.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2797091473.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2311970800.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2397236802.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2001079033.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2810418995.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2738453835.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2284307888.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2042061481.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.1991839967.000002921161C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/en-us/weather/topstories/us-weather-super-el-nino-to-bring-more-flooding-and-win	explorer.exe, 00000016.00000002.2940539964.000000007900000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.1846357884.000000007900000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://windows.msn.com:443/shell?osLocale=en-GB&chosenMarketReason=ImplicitNew	explorer.exe, 00000016.00000002.2940539964.000000007900000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.1846357884.000000007900000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.msn.com/en-us/news/politics/clarence-thomas-in-spotlight-as-supreme-court-delivers-blow-	explorer.exe, 00000016.00000002.2940539964.000000007900000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.1846357884.000000007900000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://altynbe.com/content.php2f	rundll32.exe, 00000012.00000003.18689970 96.000002921161C000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0012.00000003.2415718994.000002921161C00 0.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2680109233.000 002921161C000.00000004.00000020.00020000 .00000000.sdmp, rundll32.exe, 00000012.0 0000002.2938154508.000002921161C000.0000 0004.00000020.00020000.00000000.sdmp, ru ndll32.exe, 00000012.00000003.2762031046 .000002921161C000.00000004.00000020.0002 0000.00000000.sdmp, rundll32.exe, 000000 12.00000003.2797091473.000002921161C000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2311970800.00000 2921161C000.00000004.00000020.00020000.0 0000000.sdmp, rundll32.exe, 00000012.000 00003.2397236802.000002921161C000.000000 04.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2001079033.00000292116 1C000.00000004.00000020.00020000.0000000 0.sdmp, rundll32.exe, 00000012.00000003. 2810418995.000002921161C000.00000004.000 00020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2738453835.0000029 21161C000.00000004.00000020.00020000.000 00000.sdmp, rundll32.exe, 00000012.00000 003.2284307888.000002921161C000.00000004 .00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.1842659886.000002921161C 000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.1882552320.0 00002921161C000.00000004.00000020.000200 00.00000000.sdmp, rundll32.exe, 00000012 .00000003.2042061481.000002921161C000.00 000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.19918399 67.000002921161C000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0012.00000003.1867444760.000002921161C00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://anikvan.com/api/azuret.php.f	rundll32.exe, 00000012.00000003.27384538 35.000002921161C000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://cdn.query.prod.cms.msn.com/cms/api/amp/binary/AA13gMeu	explorer.exe, 00000016.00000002.29405399 64.0000000007900000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1846357884.000000000790000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http:// https://cdn.query.prod.cms.msn.com/cms/api/amp/binary/AA13gTUY-dark	explorer.exe, 00000016.00000002.29405399 64.0000000007900000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1846357884.000000000790000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.rd.com/list/polite-habits-campers-dislike/	explorer.exe, 00000016.00000002.29405399 64.0000000007900000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1846357884.000000000790000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/content.phpL	rundll32.exe, 00000012.00000003.28104189 95.000002921159F000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0012.00000002.2938154508.000002921159F00 0.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2762031046.000 002921159F000.00000004.00000020.00020000 .00000000.sdmp, rundll32.exe, 00000012.0 0000003.2797091473.000002921159F000.0000 0004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://altynbe.com/	rundll32.exe, 00000012.00000003.18674447 60.000002921161C000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://android.notify.windows.com/iOS	explorer.exe, 00000016.00000002.29457342 91.000000000C5AA000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1859052974.000000000C5AA00 0.00000004.00000001.00020000.00000000.sdmp	false		high

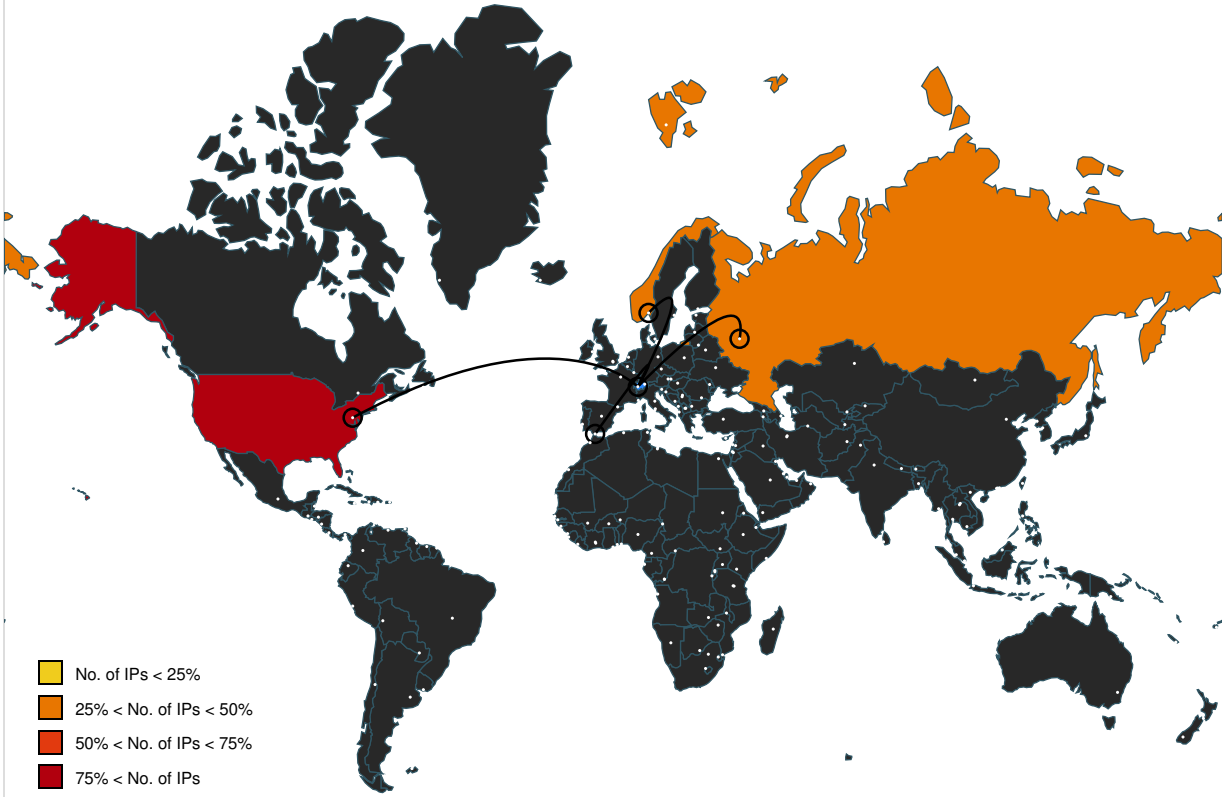
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://anikvan.com/d	rundll32.exe, 00000012.00000003.2001079033.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.1882552320.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2042061481.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.1991839967.000002921161C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azurent.php	rundll32.exe, 00000012.00000003.2797091473.000002921161C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://altynbe.com/api/azureontent.phpMfE	rundll32.exe, 00000012.00000003.2001079033.000002921161C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://img.s-msn.com/tenant/amp/entityid/AAbC0oi.img	explorer.exe, 00000016.00000000.1846357884.00000000078AD000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000002.2940539964.00000000078AD000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azurep1j	rundll32.exe, 00000012.00000003.2415718994.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2680109233.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2397236802.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2762031046.000002921163E000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2797600040.000002921163E000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2738453835.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2491436893.000002921163E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://outlook.com_	explorer.exe, 00000016.00000002.2945734291.000000000C5AA000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.1859052974.000000000C5AA000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://www.rd.com/newsletter/?int_source=direct&int_medium=rd.com&int_campaign=nlrda_20221001_toppe	explorer.exe, 00000016.00000002.2940539964.0000000007900000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.1846357884.0000000007900000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://workspacin.cloud/live/J5	explorer.exe, 00000016.00000002.2947027390.000000000CA7C000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/content.phpA	rundll32.exe, 00000012.00000003.2284190577.00000292115AE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/en-us/news/world/agostini-krausz-and-l-huillier-win-physics-nobel-for-looking-at	explorer.exe, 00000016.00000002.2940539964.0000000007900000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.1846357884.0000000007900000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/content.phpLgF	rundll32.exe, 00000012.00000003.2762031046.000002921161C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azure.php	rundll32.exe, 00000012.00000003.2397236802.000002921161C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/content.php&j	rundll32.exe, 00000012.00000003.2311970800.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2491436893.000002921163E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://boriz400.com/qa	rundll32.exe, 00000012.00000003.2415718994.000002921161C000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2397236802.000002921161C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/en-us/news/us/when-does-daylight-saving-time-end-2023-here-s-when-to-set-your-cl	explorer.exe, 00000016.00000002.2940539964.00000000078AD000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerpoint.office.comcember	explorer.exe, 00000016.00000002.29457342 91.000000000C5AA000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1859052974.000000000C5AA00 0.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://workspacin.cloud/	explorer.exe, 00000016.00000002.29457342 91.000000000C54A000.00000004.00000001.00 020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://altynbe.com/X	rundll32.exe, 00000012.00000003.26801092 33.000002921161C000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/en-us/money/personalfinance/no-wonder-the-american-public-is-confused-if-you-re-	explorer.exe, 00000016.00000002.29405399 64.0000000007900000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1846357884.000000000790000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azurepP	rundll32.exe, 00000012.00000003.24157189 94.000002921161C000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0012.00000003.2397236802.000002921161C00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.micro	explorer.exe, 00000016.00000000.18501428 84.0000000009B60000.00000002.00000001.00 040000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1847476814.000000000872000 0.00000002.00000001.00040000.00000000.sdmp, explorer.exe, 00000016.00000002.2941807069.000 0000007F40000.00000002.00000001.00040000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://altynbe.com/d	rundll32.exe, 00000012.00000003.26801092 33.000002921161C000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://anikvan.com/api/azure==	rundll32.exe, 00000012.00000003.26801092 33.00000292115EE000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0012.00000003.1882552320.00000292115EF00 0.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2415718994.000 00292115EF000.00000004.00000020.00020000 .00000000.sdmp, rundll32.exe, 00000012.0 0000003.2311970800.00000292115EF000.0000 0004.00000020.00020000.00000000.sdmp, ru ndll32.exe, 00000012.00000002.2938154508 .00000292115EF000.00000004.00000020.0002 0000.00000000.sdmp, rundll32.exe, 000000 12.00000003.2001079033.00000292115EE000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.1991839967.00000 292115EF000.00000004.00000020.00020000.0 0000000.sdmp, rundll32.exe, 00000012.000 00003.2762031046.00000292115EF000.000000 04.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2284190577.00000292115 EF000.00000004.00000020.00020000.0000000 0.sdmp, rundll32.exe, 00000012.00000003. 2042061481.00000292115EF000.00000004.000 00020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2738816096.0000029 2115EF000.00000004.00000020.00020000.000 00000.sdmp, rundll32.exe, 00000012.00000 003.2397236802.00000292115EF000.00000004 .00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2810418995.00000292115EF 000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2797091473.0 0000292115EF000.00000004.00000020.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/content.phpMfE	rundll32.exe, 00000012.00000003.19918399 67.000002921161C000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://altynbe.com/5~	rundll32.exe, 00000012.00000003.18426598 86.000002921161C000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://windows.msn.com:443/shellv2?osLocale=en-GB&chosenMarketReason=ImplicitNew	explorer.exe, 00000016.00000002.29405399 64.0000000007900000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1846357884.000000000790000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://boriz400.com/	rundll32.exe, 00000012.00000003.23972368 02.00000292115AE000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/en-us/lifestyle/travel/i-ve-worked-at-a-campsite-for-5-years-these-are-the-15-mi	explorer.exe, 00000016.00000002.29405399 64.0000000007900000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1846357884.000000000790000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://api.msn.com/q	explorer.exe, 00000016.00000000.18479162 03.00000000097D4000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000002.2942821965.00000000097D400 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://api.msn.com/v1/news/Feed/Windows?activityId=0CC40BF291614022B7DF6E2143E8A6AF&timeOut=5000&oc	explorer.exe, 00000016.00000002.29405399 64.0000000007900000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1846357884.000000000790000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azurepjB	rundll32.exe, 00000012.00000003.24157189 94.000002921161C000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0012.00000003.2311970800.000002921161C00 0.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2397236802.000 002921161C000.00000004.00000020.00020000 .00000000.sdmp, rundll32.exe, 00000012.0 0000003.2284307888.000002921161C000.0000 0004.00000020.00020000.00000000.sdmp, ru ndll32.exe, 00000012.00000003.2491436893 .000002921163E000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://altynbe.com/api/azureure	rundll32.exe, 00000012.00000003.28104189 95.000002921161C000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/en-us/lifestyle/lifestyle-buzz/biden-makes-decision-that-will-impact-more-than-1	explorer.exe, 00000016.00000002.29405399 64.0000000007900000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1846357884.000000000790000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://assets.msn.com/staticsb/statics/latest/traffic/Notification/desktop/svg/RoadHazard.svg	explorer.exe, 00000016.00000000.18463578 84.0000000007900000.00000004.00000001.00 020000.00000000.sdmp	false		high
http://https://cdn.query.prod.cms.msn.com/cms/api/amp/binary/AA13gMeu-dark	explorer.exe, 00000016.00000002.29405399 64.0000000007900000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1846357884.000000000790000 0.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.msn.com/en-us/money/personalfinance/13-states-that-don-t-tax-your-retirement-income/ar-A	explorer.exe, 00000016.00000002.29405399 64.0000000007900000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.1846357884.00000000078AD00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.1846357884.000 0000007900000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 00000016.0 0000002.2940539964.00000000078AD000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://https://altynbe.com/=~	rundll32.exe, 00000012.00000003.26801092 33.000002921161C000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0012.00000003.2762031046.000002921161C00 0.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000012.00000003.2738453835.000 002921161C000.00000004.00000020.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io/n	rundll32.exe, 00000012.00000003.20010790 33.000002921161C000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0012.00000003.1991839967.000002921161C00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/content.php4	rundll32.exe, 00000012.00000003.23119708 00.000002921161C000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io/api/azurep&j	rundll32.exe, 00000012.00000003.28106182 43.000002921163E000.00000004.00000020.00 020000.00000000.sdmp, rundll32.exe, 0000 0012.00000003.2797600040.000002921163E00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://altynbe.com/api/azurep	rundll32.exe, 00000012.00000003.26801092 33.000002921161C000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/en-us/news/topic/breast%20cancer%20awareness%20month?ocid=winp1headerevent	explorer.exe, 00000016.00000002.2940539964.0000000007900000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.1846357884.0000000007900000.00000004.00000001.00020000.00000000.sdmp	false		high
http://upx.sf.net	Amcache.hve.9.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.164.68.73	anikvan.com	Gibraltar		29632	NASSIST-ASGI	true
138.124.183.215	altynbe.com	Norway		8983	NOKIA-ASFI	true
104.21.16.155	workspacin.cloud	United States		13335	CLOUDFLARENETUS	true
3.69.236.35	ae1f8849daaac4ee6b80681872ab88b9-1762121307.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
91.194.11.183	boriz400.com	Russian Federation		42994	HQservCommunicationSolutionsIL	true
54.175.181.104	ae97372e4f96e4d1299fbaeb7130b656-1584023256.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1439879
Start date and time:	2024-05-11 00:03:08 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 7m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	upfilles.dll.dll (renamed file extension from exe to dll)
Original Sample Name:	upfilles.dll.exe
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@32/17@8/6
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, WMIADAP.exe, SIHClient.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.168.117.173, 20.189.173.20
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, ocsp.digicert.com, login.live.com, slscr.update.microsoft.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus15.westus.cloudapp.azure.com, ctldl.windowsupdate.com, umwatson.events.data.microsoft.com, fe3cr.delivery.mp.microsoft.com
- HTTPS proxy raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- 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 NtEnumerateKey calls found.
- 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.
- VT rate limit hit for: upfilles.dll.dll

Simulations

Behavior and APIs

Time	Type	Description
00:04:08	API Interceptor	1500037x Sleep call for process: rundll32.exe modified
00:04:08	API Interceptor	1x Sleep call for process: loaddll64.exe modified
00:04:11	API Interceptor	4x Sleep call for process: WerFault.exe modified
00:04:51	API Interceptor	2619129x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_964e80f5d1a5f925558a7e6299462efecb949df_9db0ef65_6fb130ca-cac1-4736-bec2-e227247d8b1e\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7695669651831538
Encrypted:	false
SSDEEP:	96:0SFi/iSyKyosj+4RvNxrfNrQXIDcQOc6ncECcw3l+XaXz+HbHgSQgJjZh88Wpoxf:3ciSyoA80wjIx8jbyzuiFeZ24lO83l
MD5:	F38F1F5A2799280E9AE9ECAED3D4D7F2
SHA1:	614B13F3576A06B0A5D66A28720AD52CD48F64F1
SHA-256:	73EACA5144E5222EA3859908633BE224CDF2CD699D28056A5D123197108AFA1D
SHA-512:	B9504BAE2E55AB063A7D732A66DBD0739F937C3A3F9B1ED05B2C9E54966B1D4A4FF1AF7BF0FA1B5BC023C7BFA404DDCCC9217463CBFCCB67275A9DBB3F848250
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.=.1.3.3.5.9.8.5.2.2.4.8.7.5.7.2.1.5.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.5.9.8.5.2.2.4.9.1.1.6.5.9.8.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.f.b.1.3.0.c.a.-.c.a.c.1.-.4.7.3.6.-.b.e.c.2.-.e.2.2.7.2.4.7.d.8.b.1.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.f.f.0.0.0.3.c.-.c.f.1.a.-.4.8.1.3.-.9.0.a.4.-.5.5.b.6.8.a.f.9.f.4.1.0.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.u.p.f.i.l.l.e.s...d.l.l...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.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.c.7.8.-.0.0.0.1.-.0.0.1.4.-.8.e.2.1.-.0.7.f.b.2.5.a.3.d.a.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.0.!.0.0.0.0.d.d.3.9.9.a.e.4.6.3.0.3.3.4.3.f.9.f.0.d.a.1.8.9.a.e.e.1.1.c.6.7.b.d.8.6.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_964e80f5d1a5f925558a7e6299462efecb949df_9db0ef65_d9b8934c-437b-450d-af46-0185962b24b1\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7695284270582192
Encrypted:	false
SSDEEP:	96:DgFPd/ifyKyOsj+4RvNxrfNrQXIDcQOc6ncECcw3l+XaXz+HbHgSQgJjZh88Wpo3:s11ifyOA80wjIx8jbyzuiFeZ24lO83D
MD5:	2A79D4F0CC409452333A8DDF84450AEF
SHA1:	512CBEAAAC2972AE331C435F33652DABEA99A541
SHA-256:	3B527751CA5679B2B05D430B17ADDE2A98AFCC30216D6AA11E58AFF116A824B0
SHA-512:	9B02987593193A773237874A8B64ED4910787AF41B8B8ABCCC5DBA27DF4A1CFE6DC316B2342075BCB51ADB9B0D7033C8AEE7CBCC8867DFD0860E46D5A3FFFA6
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.=.1.3.3.5.9.8.5.2.2.4.5.2.8.4.4.3.6.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.5.9.8.5.2.2.4.5.5.9.6.9.2.5.5.....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.=.d.9.b.8.9.3.4.c.-.4.3.7.b.-.4.5.0.d.-.a.f.4.6.-.0.1.8.5.9.6.2.b.2.4.b.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.=.1.a.7.5.8.8.6.c.-.1.e.1.4.-.4.9.7.7.-.a.4.1.a.-.1.2.a.6.4.d.0.0.c.9.b.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.u.p.f.i.l.l.e.s...d.l.l...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.7.4.-.0.0.0.1.-.0.0.1.4.-.9.1.1.3.-.3.8.f.9.2.5.a.3.d.a.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.0.!.0.0.0.0.d.d.3.9.9.a.e.4.6.3.0.3.3.4.3.f.9.f.0.d.a.1.8.9.a.e.e.1.1.c.6.7.b.d.8.6.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_dc8a9dd96bb43aa654aa29aa9f464ac6a31131f_9db0ef65_7dc7f057-dc81-4d91-9caa-bd8701d223a3\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7695293488830603

Encrypted:	false
SSDEEP:	96:CcxgFF3/iOyKyZsj+4RvNxrfKQXIDcQOc6ncETcw3CCXaXz+HbHgSQgJjZh88Wp8:FgviOyZK0wjpFjbyzuiFeZ24lO83
MD5:	02C2AE579A388FFA4C5C6A5104F49832
SHA1:	0C660AE3539AE95EDF65C53088E9DA7EB5DFFEC9
SHA-256:	C313D051688A264AD7778F15CEC6ECB0D2FA908EA92D9134E25ED80B3B43C826
SHA-512:	A0A17281B979ACB45169A5C79673EC67EEC58F73B21E9D325CE34BD1630D7DBF459BF7AA4DCCE803D8D4842130BCD62AEE4F3822E8A75FA2770905BD285D08 30
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.=.1.3.3.5.9.8.5.2.2.4.8.5.5.9.7.4.2.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l. o.a.d.T.i.m.e.=.1.3.3.5.9.8.5.2.2.4.8.9.9.7.2.4.3.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.d.c.7.f.0.5.7.-.d.c.8.1.-.4.d.9.1.-.9.c.a.a.-.b.d.8.7.0. 1.d.2.2.3.a.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.=.0.b.5.f.a.4.a.6.-.8.4.c.8.-.4.1.2.c.-.b.8.1.1.-.e.9.d.8.7.2.5.2.d.c.7.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p. p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.u.p.f.i.l.l.e.s...d.l.l...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.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.c.6.8.-.0.0.0.1.- .0.0.1.4.-.0.4.1.7.-.0.6.f.b.2.5.a.3.d.a.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.d.d.3.9.9.a. e.4.6.3.0.3.3.4.3.f.9.f.0.d.a.1.8.9.a.e.e.1.1.c.6.7.b.d.8.6.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_dc8a9dd96bb43aa654aa29aa9f464ac6a31131f_9db0ef65_8641b0ad-46f6-452c-a496-10d58d4ec871\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7695999953173611
Encrypted:	false
SSDEEP:	96:TEF1ks0/idyKygsj+4RvNxrfKQXIDcQOc6ncETcw3CCXaXz+HbHgSQgJjZh88Wp8:o3CidygK0wjpFjbyzuiFeZ24lO83
MD5:	F9DA4317B3745718F8A31BB61F06A4F4
SHA1:	9BD89B72FF6CD9493B7343C4A720B403B54D0439
SHA-256:	072151E64254174294A716437E4F986EC8336BAC545EBEA5D71EC5A481A00DBD
SHA-512:	D2E3D37FAB0EB27FDEAA9A17C253B5D225EA96CD53D898A9F7A8A829D2D6B887E0139387DF6CDA03D85A7E2E8595025E08032A65822C12B65E124144B35837A C
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.=.1.3.3.5.9.8.5.2.2.4.2.3.7.7.9.6.8.2.....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.=.1.3.3.5.9.8.5.2.2.4.2.7.3.7.3.4.3.5.....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.=.8.6.4.1.b.0.a.d.-.4.6.f.6.-.4.5.2.c.-.a.4.9.6.-.1.0.d.5.8. d.4.e.c.8.7.1.....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.=.e.a.0.2.e.b.5.a.-.0.8.a.0.-.4.c.3.1.-.b.1.3.9.-.4.4.8.1.7.4.2.9.8.e.a.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p. p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.u.p.f.i.l.l.e.s...d.l.l...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.b.4.-.0.0.0.1.- .0.0.1.4.-.0.d.f.7.-.6.b.f.7.2.5.a.3.d.a.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.d.d.3.9.9.a. e.4.6.3.0.3.3.4.3.f.9.f.0.d.a.1.8.9.a.e.e.1.1.c.6.7.b.d.8.6.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri May 10 22:04:02 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	66070
Entropy (8bit):	1.5462375465383378
Encrypted:	false
SSDEEP:	96:5u8hjNE3e2neSVUa52sl4GbfhHoi7M9UUACGcKutR1ZfE0FXtpqgJbqStCSqjWIF:XhjNi2OM+UAtq1ZfNTqgwStCS9ngz
MD5:	677694119DA44E5FEC7BF1C1317E830B
SHA1:	4FEB41E3E2792D4305F3FD66F5EE17E8BFFDA32D
SHA-256:	13C9DE6CF736408ECF3F5D8B186442A3381B005B307FDBD5DCEB114A627866FB
SHA-512:	000B790E53523A6DFE23A290EFD228BFF0E399927D925B880663ED99F0F3E07957C357E346C4976419B62BC34EC43367BE19E3CA39663B65BD3A6E16CDCE282
Malicious:	false
Preview:	MDMP..a..... .....>f.....$.....T.....8.....T.....p.....eJ.....Lw..... .....T.....>f.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .S.u.m.m.e.r. .T.i.m.e..... .....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8534
Entropy (8bit):	3.6939797702013397
Encrypted:	false

SSDEEP:	192:R6l7wVeJqdgkmE6Yo8N4LgmfWP3pry89bU66Wf088m:R6lXJqakmE6YLegmfWPRU6DfR
MD5:	80B9B0AFA9ABA69B9A78557C448086C5
SHA1:	B99101A8A598F674B85334D5F8A0609AC22631E6
SHA-256:	9968C12422E570B5EE4916B7EDF4BC0240E72DE23F62EF10630EC4B1E51814FF
SHA-512:	8D2CBE94CDDBA9C7F4FDD42B91E690533542BB23B8DD38FD258D3CC44585D6C07E12DA68A06CC179B1B8C7D8C3A8F400316A4787D58FB980DD530F34F2BAE69
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.>.1.9.0.4.5.<./.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.>.1.9.0.4.1...2.0.0.6...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.2.0.0.6.<./.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.>.2.0.5.7.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.3.2.4.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E1D.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4777
Entropy (8bit):	4.477202967569579
Encrypted:	false
SSDEEP:	48:cvIwWl8zssJg771l99aWpW8VY+Ym8M4JCNCF0laFtyq85mQCy8ptSTSLd:uIjfql7+b7VeJilCGT8poOLd
MD5:	5D367A225C41966DC6550185A90DAE6F
SHA1:	101CC4DF6477453EA9552B5AD0EE1273F1599AEA
SHA-256:	E6997AC198F3DBE27F9915E0C4A3CC5E65654C6536885480C9BC6EF40290C190
SHA-512:	EDF7487656C3685EFE40BEAB794203DDBF95DD49E14CA56E27EAC8BD88B5CCE0BFF9C5555D329990288C05738F40CF731B5EE9D15DB3800A90DCA5F80C5D4F8
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="19045" />.. <arg nm="vercsdbld" val="2006" />.. <arg nm="verqfe" val="2006" />.. <arg nm="csdbld" val="2006" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="2057" />.. <arg nm="geoid" val="223" />.. <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="317586" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="409

C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri May 10 22:04:05 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	58190
Entropy (8bit):	1.605256614606473
Encrypted:	false
SSDEEP:	192:0VrYrCpCzQOMAsu+Qiqwxay+QsK0QRAQh:2E1TpoQi1aZQsK/Rp
MD5:	CAAA37C00D8ECF6FA5FC4FA2A30BD2FA
SHA1:	2F9D061ED037ECE51B72AC937A99813073410435
SHA-256:	ECA00EFCB890B105FA3A548999F1E7A161FD7BDB5ED7B1F2FF2240DF570C41E2
SHA-512:	9432BA4BCEB6E8A6D56DB1CBD256C7A1C3835413B22B4CEC7A7D8D7FACC8A85CF7E981CDC802E9A7001EB67285401042ED97471A5617B1D8BC220A145DD928C2
Malicious:	false
Preview:	MDMP..a..... .....>f.....)..... T.....8..... T..... V..... T..... @..... eJ..... Lw..... T.....t....>f..... 0..... W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... W... .E.u.r.o.p.e. .S.u.m.m.e.r. .T.i.m.e..... 1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8534
Entropy (8bit):	3.6966319113948383
Encrypted:	false
SSDEEP:	192:R6l7wVeJRBAmS6YojN4LgmfWfiwsprRC89br4Wf9vZm:R6lXJXAmS6YEegmfWqP7rxfi
MD5:	B607A2EB5584FD30993D12ABB2C4DF8A

SHA1:	F2E1E2CE69FB5F3AB9850FF3A56668B6DFAE0AFF
SHA-256:	DC1BDEED634E5907DFD137282558057ED000A00CD7BABC1ABC665D6B47410064
SHA-512:	249030B4D7B167C51DA04101F483BFE2D977EDE4D0DBAF6E45720002D56785033391999DCBE0591289B8DE51E15D1C1ADBCE641A4472471D0A4B869CED69DD 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.>.1.9.0.4.5.<./.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.>.1.9.0.4.1...2.0.0.6...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-. 1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.2.0.0.6.<./.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.>.2.0.5.7.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i. d.>.6.5.1.6.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3919.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4777
Entropy (8bit):	4.480227848947886
Encrypted:	false
SSDEEP:	48:cvIwWl8zssJg771l99aWpW8VYsYm8M4JCNCF0saFmjyq85mQCrAptSTSDd:uIjfqI7+b7VEJi8jGfpoODd
MD5:	76611ED68AE98A3C1C5418DA42AD9839
SHA1:	E56614DC31056975565348CCA2BC464DC61B1657
SHA-256:	1E7C757B8CED61BB0960A6FD8EE447BE3D82DF516B6DBF0CD4E9DD3CD465F897
SHA-512:	1852341A694CC87F021633950EA49ECE0FDC5D470769097BE801C9F5F525F77E075FF0F4FC9BAE3266E303161AB520D0DEFF756C4B6DF3F6CF50F20AD73A052(
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="19045" />.. <arg nm="vercsdbld" val="2006" />.. <arg nm="verqfe" val="2006" />.. <arg nm="csdbld" val="2006" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="2057" />.. <arg nm="geoid" val="223" />.. <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="317586" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="409

C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri May 10 22:04:08 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	57494
Entropy (8bit):	1.6234250646337964
Encrypted:	false
SSDEEP:	192:duYrC6W3OMlUsn9pHz+bF7frc/wHGpzp/iaBReJd5U6:rhZgV9lxXpzp/9jePL
MD5:	66F2A3C376DA0D558312FF6110D838C3
SHA1:	834B317025A81AA5E7F00DF4430D56F7D760645B
SHA-256:	562F917C37C8D1E62F2E934483DEF3B9032D3EDBDE40154FD19E1CEA1BE2BAF2
SHA-512:	58CC96682B33937C6CBB1E4CA8C0F7A07A37CD327DF704A9149CEAD1272E8F4C2539691B2C8FA46B75BB017353F11C02BD129EFE4159EE3081DF67D534CB97 C
Malicious:	false
Preview:	MDMP..a..... .....>f.....).....T.....8.....T.....T.....@.....eJ.....Lw..... .....T.....h....>f.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .S.u.m.m.e.r. .T.i.m.e..... .....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8522
Entropy (8bit):	3.6962697567258553
Encrypted:	false
SSDEEP:	192:R6l7wVeJtabmV6Y7pGgmfWP3prM89b+rWfxKm:R6lXJwbmV6YFGgmfWPT+6fd
MD5:	B71FE5E91F46A2F6E80793B28555315E
SHA1:	52F0EE991F743BEA0995768C5AA075635A979098
SHA-256:	7F8F6E795A696CA77E094A9664C2A6B795FFB3C2E9A5A6AEF1ED303C408F7EA0

SHA-512:	5CE960EE43F0BD8BEE75A7688B62FD8BD51F4CE59AF84251C28867D7FD5E54FF5E03D2D159A5C36D8B04415FB04CF4EA130D1036D1D8DC564B5B2F961FFE02 03
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.>.1.9.0.4.5.<./.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.>.1.9.0.4.1...2.0.0.6...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-. 1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.2.0.0.6.<./.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.>.2.0.5.7.<./.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.>.7.2.7.2.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4648.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4777
Entropy (8bit):	4.478653683433715
Encrypted:	false
SSDEEP:	48:cvIwWl8zssJg771l99aWpW8VYpYm8M4JCNCF0laFniyq85mQCypptSTS6d:uljfqI7+b7V1JilVGTppoO6d
MD5:	DA7D9A451274291EFD3755DC8FC3A141
SHA1:	51E42DA26BBC94435F94EFDBDF8A242CC744E57C
SHA-256:	821799E5797BB8E3BCB45C123C170C09004DB0C21BB4FC46A6F6A99DE66FFC12
SHA-512:	1AADD5F0D59B95756B48DFE2F6F95D358774409C5E209449411050C86A5F3990AE52D7AA1BBDD93063D712B6CB0DC84BE37183381300442312 8DF6949663B53A
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="19045" />.. <arg nm="vercsdbld" val="2006" />.. <arg nm="verqfe" val="2006" />.. <arg nm="csdbld" val="2006" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="2057" />.. <arg n m="geoid" val="223" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtyp e" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="317586" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.78 9.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="409

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri May 10 22:04:08 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	54894
Entropy (8bit):	1.6839237359198767
Encrypted:	false
SSDEEP:	96:59S8veE3+XuQRawUKUCGsV3bBvgoi7MxpnZ0mK1NX7RT9bCmYhJbqmpx5OqWRW/F:diYrCrOMzuJXeDwwx5OLIH9EyXh
MD5:	A837E0375D7983509A56860346CFCC15
SHA1:	F75FAE2A056C6FEF8D8F1D700F3412213DFFFB2D
SHA-256:	205CD9270682DC17A83E8D40610371F3ED964DD319E67BDBA4BE1780DF36D02F
SHA-512:	DAD398EB6A465DF561E9F4A51FD2D414C84CFFB7F34BC06FEE2515B88EDCAC48978359ADA324F8A441AE9304221089DF081651A0CC5B770D121A04ED586B5A 4A
Malicious:	false
Preview:	MDMP..a..... ....>f.....)..........T.......8..........T..............v..........T..........@.....eJ.....Lw..... .....T.....x....>f.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .S.u.m.m.e.r. .T.i.m.e..... .....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8522
Entropy (8bit):	3.6958245523678235
Encrypted:	false
SSDEEP:	192:R6l7wVeJoigmd6Y7GGgmfWfiwsprH89b+vWfuKm:R6lXJdgmd6Y6GgmfWq2+ef6
MD5:	57975B44072D1C9B3E80DB2266217745
SHA1:	A9CF9831C70448BFE57EB598D192F042A2AE3A6D
SHA-256:	415AD9CE27C4A61A389B2D2AE85DF89BB06FEFD9971BDB3399CAE445E58B8910
SHA-512:	93854E117CDB0F89602B01AA667CE2E15D7607242C6EC26A4B7060F5FCB7EB905ADB72A73E979F8B35E01DA8F21F8CEE3A99D7FA40DD04ABBBD3428F6F83C2 12
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.>.1.9.0.4.5.<./.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.>.1.9.0.4.1...2.0.0.6...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.2.0.0.6.<./.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.>.2.0.5.7.<./.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.>.7.2.8.8.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4704.tmp.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4777
Entropy (8bit):	4.481691067176541
Encrypted:	false
SSDEEP:	48:cvIwWl8zssJg771l99aWpW8VYSYm8M4JCNCF0saFBwtjyq85mQCrdptSTSNd:uIjfqI7+b7VCJiP0GqpoONd
MD5:	243DA7FD47223239375D054C23BDE13D
SHA1:	01345C28EFD562EEDE44945D9F8B54A30951ABC4
SHA-256:	CF4636B318E7DCECACDC72437D290E86C0501BCA90B77EE7585C1C837614D3D3
SHA-512:	9BCE637D0F2AA10F4FD3BE688AFC8B97DC87CD20E03157250D55EC6368C6E353BB80A712BA982C01CA00B082C593634FA65DC3295A1EF8F9DCAA3C69330CC3F
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="19045" />.. <arg nm="vercsdbld" val="2006" />.. <arg nm="verqfe" val="2006" />.. <arg nm="csdbld" val="2006" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="2057" />.. <arg nm="geoid" val="223" />.. <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="317586" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="409

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\System32\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1835008
Entropy (8bit):	4.46640558354698
Encrypted:	false
SSDEEP:	6144:/IXfpi67eLPU9skLmb0b4zWSPKaJG8nAgejZMMhA2gX4WABl0uNcdwBCswSb9:wXD94zWlLZMM6YFHa+9
MD5:	B7B3B5CD7790EDF0686FF777BA5097D3
SHA1:	ED234CE4B519238F46F4AA9519B3C51AFB301F20
SHA-256:	221475E4ACF30CBC675FA384CAE2C143B9C04EF7B913D8D65B0052080F31D095
SHA-512:	2F5813E176688BB57E91FD992373740377CDE50F0EBF56BD906A17D6325F158525F85FA13581310839B2EB9219FD5E6F03A3DE3E3E9A32CF3DAAC2D1BAE2683
Malicious:	false
Preview:	regf6...6....\.Z..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e....c...b...#.....c...b...#.....c...b...#.....rmtm...%..... ....U..... .....

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	7.38766220411242
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	upfilles.dll.dll
File size:	520'704 bytes
MD5:	ccb6d3cb020f56758622911ddd2f1fcb
SHA1:	4a013f752c2bf84ca37e418175e0d9b6f61f636d
SHA256:	f4cb6b684ea097f867d406a978b3422bbf2ecfea39236bf3ab99340996b825de
SHA512:	6ed929967005eaa6407e273b53a1fedcb2b084d775bed17272fd05b1ce143dbf921ac201246dfbfdbe663c7351e44c12f162e6f03343548b69b5d4598bb3492e

SSDEEP:	12288:8XG3MpAOIQ1LjbJFqzqUtYP4VnRk62yoK2:SpAOfFJlq/Py8K2
TLSH:	4AB4BE4A37A80CB6E867C17D88634705E3B27D610761C6DF1290536F9F3BBD2663AB12
File Content Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....C.s.". .". .". .D.!.". .D.!o". .J.!.". .J.!.". .J.!.". tK.!.". .D.!.". .D.!.". .". q". tK.!.". tK.!.". tK.!.". tK? .". ."W .".

File Icon

Icon Hash:	7ae282899bbab082

Static PE Info

General

Entrypoint:	0x18000e1c0
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	HIGH_ENTROPY_VA
Time Stamp:	0x5C24FE09 [Thu Dec 27 16:30:01 2018 UTC]
TLS Callbacks:	0x80020fe0, 0x1
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	90ad3b5a283c3a333bb222c03419fb76

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
dec eax
mov dword ptr [esp+08h], ebx
dec eax
mov dword ptr [esp+10h], esi
push edi
dec eax
sub esp, 20h
dec ecx
mov edi, eax
mov ebx, edx
dec eax
mov esi, ecx
cmp edx, 01h

Instruction
jne 00007F611CBAF4F7h
call 00007F611CBAF8D0h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007F611CBAF384h
int3
int3
int3
dec eax
mov dword ptr [esp+10h], ebx
dec eax
mov dword ptr [esp+18h], ebp
push esi
push edi
inc ecx
push esi
dec eax
sub esp, 10h
xor ecx, ecx
mov dword ptr [00029DFEh], 00000002h
xor eax, eax
mov dword ptr [00029DEEh], 00000001h
cpuid
inc esp
mov edx, ecx
inc esp
mov ecx, edx
xor ecx, 444D4163h
xor edx, 69746E65h
mov ebp, ebx
inc ebp
xor ebx, ebx
xor ebp, 68747541h
inc esp
mov eax, ebx
or ebp, edx
inc esp
mov esi, eax
or ebp, ecx
inc ecx
xor ecx, 49656E69h
inc ecx
xor eax, 756E6547h
inc ecx
lea eax, dword ptr [ebx+01h]
xor ecx, ecx
inc ecx
xor edx, 6C65746Eh
cpuid

Instruction
inc ebp
or eax, ecx
mov dword ptr [esp], eax
inc ebp
or eax, edx
mov dword ptr [esp+04h], ebx
mov esi, ecx
mov dword ptr [esp+08h], ecx
mov edi, eax
mov dword ptr [esp+00h], edx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x36de0	0xbc	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x36e9c	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3e000	0x1238	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x3b000	0x22bc	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3c400	0x3278	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x40000	0x8fc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x31570	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x316d0	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x315d0	0x100	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x25000	0x3d8	.rdata
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	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x23a99	0x23c00	87bfc32636bf93aa5ba6a79278de1d82	False	0.5472779173951049	data	6.420263931637599	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x12b20	0x12c00	0f7e92ec4b27ef7a718d78d4d512f916	False	0.4034114583333333	OpenPGP Secret Key Version 3	4.778349716646358	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x38000	0x2b34	0x1600	a4dd3c567a44787ef36b75c1461eadc7	False	0.189453125	data	3.77323134284555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x3b000	0x22bc	0x2400	4b6b0ab05d617b8443d04115ebcf4698	False	0.4678819444444444	data	5.261331885690949	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3e000	0x1238	0x1400	262a27cc3c07916543c338d007e971a7	False	0.3376953125	data	4.197268760185116	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x40000	0x8fc	0xa00	029935b97db1b1dda5ddd384d84aface	False	0.52734375	data	5.178504761959821	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
hVr	0x41000	0x43000	0x42e00	b359e2ed16a1c00b78e0035c276c8cf4	False	0.9683703271028037	data	7.985612673503669	IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
REGISTRY	0x3e6c0	0xc	ASCII text, with CRLF line terminators	English	United States	1.6666666666666667
REGISTRY	0x3e598	0x125	ASCII text, with CRLF line terminators	English	United States	0.7747440273037542
REGISTRY	0x3e6d0	0x1fc	ASCII text, with CRLF line terminators	English	United States	0.5866141732283464
TYPELIB	0x3e8d0	0x7b8	data	English	United States	0.31983805668016196
RT_STRING	0x3f088	0x2c	data	English	United States	0.5681818181818182
RT_VERSION	0x3e200	0x398	OpenPGP Public Key	English	United States	0.45652173913043476
RT_MANIFEST	0x3f0b8	0x17d	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States	0.5931758530183727

Imports

DLL	Import
KERNEL32.dll	UnmapViewOfFile, FreeLibrary, GetModuleFileNameW, GetModuleHandleW, GetProcAddress, LoadLibraryExW, LoadResource, SizeofResource, FindResourceW, lstrcmpiW, MultiByteToWideChar, MapViewOfFile, EncodePointer, EnterCriticalSection, LeaveCriticalSection, GetThreadLocale, SetThreadLocale, CreateFileW, GetFileSizeEx, CreateFileMappingW, GetCurrentThreadId, GetCurrentProcessId, DeleteCriticalSection, InitializeCriticalSectionEx, GetLastError, RaiseException, DecodePointer, CloseHandle, CreateEventW, OpenEventA, CreateEventA, WaitForSingleObjectEx, ResetEvent, SetEvent, WriteConsoleW, GetConsoleMode, GetConsoleCP, WriteFile, LocalAlloc, SetLastError, LocalFree, IsDebuggerPresent, OutputDebugStringW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, GetStartupInfoW, QueryPerformanceCounter, GetSystemTimeAsFileTime, InitializeSListHead, RtlPcToFileHeader, RtlUnwindEx, InterlockedFlushSList, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, ExitProcess, GetModuleHandleExW, HeapFree, HeapAlloc, HeapSize, HeapReAlloc, GetStdHandle, GetFileType, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, WideCharToMultiByte, GetEnvironmentStringsW, FreeEnvironmentStringsW, LCMapStringW, GetProcessHeap, SetFilePointerEx, GetStringTypeW, SetStdHandle, FlushFileBuffers
USER32.dll	CharNextW
ADVAPI32.dll	RegQueryInfoKeyW, RegOpenKeyExW, RegEnumKeyExW, RegDeleteValueW, RegDeleteKeyW, RegCreateKeyExW, RegCloseKey, RegSetValueExW
ole32.dll	CoTaskMemRealloc, CoTaskMemFree, CoCreateInstance, StringFromGUID2, CoTaskMemAlloc
OLEAUT32.dll	VarUI4FromStr, SysFreeString, SysAllocString, SysStringLen, LoadTypeLib, RegisterTypeLib, UnRegisterTypeLib
ntdll.dll	NtRequestWaitReplyPort, NtConnectPort, NtClose, NtRequestPort, RtlCaptureContext, RtlLookupFunctionEntry, NtCreateSection, RtlVirtualUnwind, RtlNtStatusToDosError, RtlInitUnicodeString

Exports

Name	Ordinal	Address
DllCanUnloadNow	1	0x18000b1c0
DllGetClassObject	2	0x18000b060
DllInstall	3	0x18000b350
stow	4	0x18000b1f0
DllUnregisterServer	5	0x18000b330

Possible Origin

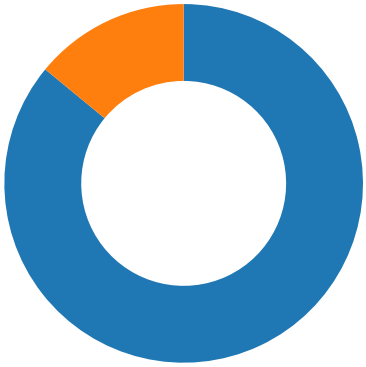
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 57

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2024 00:04:12.876111984 CEST	49745	443	192.168.2.4	91.194.11.183
May 11, 2024 00:04:12.876151085 CEST	443	49745	91.194.11.183	192.168.2.4
May 11, 2024 00:04:12.876234055 CEST	49745	443	192.168.2.4	91.194.11.183
May 11, 2024 00:04:12.884301901 CEST	49745	443	192.168.2.4	91.194.11.183
May 11, 2024 00:04:12.884325027 CEST	443	49745	91.194.11.183	192.168.2.4
May 11, 2024 00:04:13.100040913 CEST	443	49745	91.194.11.183	192.168.2.4
May 11, 2024 00:04:13.100138903 CEST	49745	443	192.168.2.4	91.194.11.183
May 11, 2024 00:04:13.150934935 CEST	49745	443	192.168.2.4	91.194.11.183
May 11, 2024 00:04:13.150954962 CEST	443	49745	91.194.11.183	192.168.2.4
May 11, 2024 00:04:13.151766062 CEST	443	49745	91.194.11.183	192.168.2.4
May 11, 2024 00:04:13.151813984 CEST	49745	443	192.168.2.4	91.194.11.183
May 11, 2024 00:04:13.153366089 CEST	49745	443	192.168.2.4	91.194.11.183
May 11, 2024 00:04:13.196130991 CEST	443	49745	91.194.11.183	192.168.2.4
May 11, 2024 00:04:13.836091995 CEST	443	49745	91.194.11.183	192.168.2.4
May 11, 2024 00:04:13.836138010 CEST	49745	443	192.168.2.4	91.194.11.183
May 11, 2024 00:04:13.836318970 CEST	443	49745	91.194.11.183	192.168.2.4
May 11, 2024 00:04:13.836368084 CEST	49745	443	192.168.2.4	91.194.11.183
May 11, 2024 00:04:13.836373091 CEST	443	49745	91.194.11.183	192.168.2.4
May 11, 2024 00:04:13.836404085 CEST	49745	443	192.168.2.4	91.194.11.183
May 11, 2024 00:04:13.836424112 CEST	443	49745	91.194.11.183	192.168.2.4
May 11, 2024 00:04:13.836445093 CEST	49745	443	192.168.2.4	91.194.11.183
May 11, 2024 00:04:13.836451054 CEST	443	49745	91.194.11.183	192.168.2.4
May 11, 2024 00:04:13.836477041 CEST	49745	443	192.168.2.4	91.194.11.183
May 11, 2024 00:04:14.160665989 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:14.160695076 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:14.160757065 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:14.161567926 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:14.161585093 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:14.349921942 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:14.349992037 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:14.633188009 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:14.633209944 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:14.633583069 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:14.633660078 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:14.633950949 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:14.680125952 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.302793026 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.302824020 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.302925110 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.302937031 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.302953005 CEST	443	49750	138.124.183.215	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2024 00:04:15.303011894 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.303020000 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.303076029 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.423475027 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.423537016 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.423574924 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.423590899 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.423614025 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.423616886 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.423635960 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.423640013 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.423652887 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.423682928 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.423687935 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.423732996 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.544538021 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.544625044 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.544735909 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.544791937 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.545012951 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.545084953 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.545223951 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.545291901 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.545304060 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.545350075 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.665793896 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.665921926 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.665981054 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.666047096 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.666162968 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.666223049 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.787254095 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.787345886 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.787383080 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.787396908 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.787437916 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.787437916 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.787859917 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.787950039 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.788012028 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.788074017 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.788597107 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.788633108 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.788666964 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.788672924 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.788682938 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.788746119 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.908390045 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.908490896 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.908793926 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.908823967 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.908847094 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.908876896 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.908876896 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:15.908888102 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:15.908951044 CEST	49750	443	192.168.2.4	138.124.183.215
May 11, 2024 00:04:16.029175997 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:16.029218912 CEST	443	49750	138.124.183.215	192.168.2.4
May 11, 2024 00:04:16.029264927 CEST	49750	443	192.168.2.4	138.124.183.215

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2024 00:04:12.655221939 CEST	61036	53	192.168.2.4	1.1.1.1
May 11, 2024 00:04:12.871501923 CEST	53	61036	1.1.1.1	192.168.2.4
May 11, 2024 00:04:13.858141899 CEST	49810	53	192.168.2.4	1.1.1.1
May 11, 2024 00:04:14.159241915 CEST	53	49810	1.1.1.1	192.168.2.4
May 11, 2024 00:04:18.686336040 CEST	59418	53	192.168.2.4	1.1.1.1
May 11, 2024 00:04:18.799472094 CEST	53	59418	1.1.1.1	192.168.2.4
May 11, 2024 00:04:19.608544111 CEST	55062	53	192.168.2.4	1.1.1.1
May 11, 2024 00:04:19.711488962 CEST	53	55062	1.1.1.1	192.168.2.4
May 11, 2024 00:04:35.505889893 CEST	52484	53	192.168.2.4	1.1.1.1
May 11, 2024 00:04:35.619683981 CEST	53	52484	1.1.1.1	192.168.2.4
May 11, 2024 00:05:43.047148943 CEST	63227	53	192.168.2.4	1.1.1.1
May 11, 2024 00:05:43.138046026 CEST	53	63227	1.1.1.1	192.168.2.4
May 11, 2024 00:06:00.977772951 CEST	57865	53	192.168.2.4	1.1.1.1
May 11, 2024 00:06:01.079061031 CEST	53	57865	1.1.1.1	192.168.2.4
May 11, 2024 00:06:08.749888897 CEST	53677	53	192.168.2.4	1.1.1.1
May 11, 2024 00:06:08.864455938 CEST	53	53677	1.1.1.1	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 11, 2024 00:04:12.655221939 CEST	192.168.2.4	1.1.1.1	0x8441	Standard query (0)	boriz400.com	A (IP address)	IN (0x0001)	false
May 11, 2024 00:04:13.858141899 CEST	192.168.2.4	1.1.1.1	0x3148	Standard query (0)	altynbe.com	A (IP address)	IN (0x0001)	false
May 11, 2024 00:04:18.686336040 CEST	192.168.2.4	1.1.1.1	0xaee4	Standard query (0)	ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io	A (IP address)	IN (0x0001)	false
May 11, 2024 00:04:19.608544111 CEST	192.168.2.4	1.1.1.1	0x69b6	Standard query (0)	anikvan.com	A (IP address)	IN (0x0001)	false
May 11, 2024 00:04:35.505889893 CEST	192.168.2.4	1.1.1.1	0x5f9f	Standard query (0)	uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io	A (IP address)	IN (0x0001)	false
May 11, 2024 00:05:43.047148943 CEST	192.168.2.4	1.1.1.1	0xc6d8	Standard query (0)	workspacin.cloud	A (IP address)	IN (0x0001)	false
May 11, 2024 00:06:00.977772951 CEST	192.168.2.4	1.1.1.1	0xc19b	Standard query (0)	uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io	A (IP address)	IN (0x0001)	false
May 11, 2024 00:06:08.749888897 CEST	192.168.2.4	1.1.1.1	0x7f64	Standard query (0)	ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 11, 2024 00:04:12.871501923 CEST	1.1.1.1	192.168.2.4	0x8441	No error (0)	boriz400.com		91.194.11.183	A (IP address)	IN (0x0001)	false
May 11, 2024 00:04:14.159241915 CEST	1.1.1.1	192.168.2.4	0x3148	No error (0)	altynbe.com		138.124.183.215	A (IP address)	IN (0x0001)	false
May 11, 2024 00:04:18.799472094 CEST	1.1.1.1	192.168.2.4	0xaee4	No error (0)	ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io	pub-ingress-aws-use1.cloud-ara.tyk.io		CNAME (Canonical name)	IN (0x0001)	false
May 11, 2024 00:04:18.799472094 CEST	1.1.1.1	192.168.2.4	0xaee4	No error (0)	pub-ingress-aws-use1.cloud-ara.tyk.io	ae97372e4f96e4d1299fbaeb7130b656-1584023256.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 11, 2024 00:04:18.799472094 CEST	1.1.1.1	192.168.2.4	0xaee4	No error (0)	ae97372e4f96e4d1299fbaeb7130b656-1584023256.us-east-1.elb.amazonaws.com		54.175.181.104	A (IP address)	IN (0x0001)	false
May 11, 2024 00:04:18.799472094 CEST	1.1.1.1	192.168.2.4	0xaee4	No error (0)	ae97372e4f96e4d1299fbaeb7130b656-1584023256.us-east-1.elb.amazonaws.com		35.172.8.165	A (IP address)	IN (0x0001)	false
May 11, 2024 00:04:18.799472094 CEST	1.1.1.1	192.168.2.4	0xaee4	No error (0)	ae97372e4f96e4d1299fbaeb7130b656-1584023256.us-east-1.elb.amazonaws.com		54.159.36.188	A (IP address)	IN (0x0001)	false
May 11, 2024 00:04:19.711488962 CEST	1.1.1.1	192.168.2.4	0x69b6	No error (0)	anikvan.com		95.164.68.73	A (IP address)	IN (0x0001)	false
May 11, 2024 00:04:35.619683981 CEST	1.1.1.1	192.168.2.4	0x5f9f	No error (0)	uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io	pub-ingress-aws-euc1.cloud-ara.tyk.io		CNAME (Canonical name)	IN (0x0001)	false
May 11, 2024 00:04:35.619683981 CEST	1.1.1.1	192.168.2.4	0x5f9f	No error (0)	pub-ingress-aws-euc1.cloud-ara.tyk.io	ae1f8849daaac4ee6b80681872ab88b9-1762121307.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
May 11, 2024 00:04:35.619683981 CEST	1.1.1.1	192.168.2.4	0x5f9f	No error (0)	ae1f8849daaac4ee6b80681872ab88b9-1762121307.eu-central-1.elb.amazonaws.com		3.69.236.35	A (IP address)	IN (0x0001)	false
May 11, 2024 00:04:35.619683981 CEST	1.1.1.1	192.168.2.4	0x5f9f	No error (0)	ae1f8849daaac4ee6b80681872ab88b9-1762121307.eu-central-1.elb.amazonaws.com		3.72.42.242	A (IP address)	IN (0x0001)	false
May 11, 2024 00:04:35.619683981 CEST	1.1.1.1	192.168.2.4	0x5f9f	No error (0)	ae1f8849daaac4ee6b80681872ab88b9-1762121307.eu-central-1.elb.amazonaws.com		35.157.36.116	A (IP address)	IN (0x0001)	false
May 11, 2024 00:05:43.138046026 CEST	1.1.1.1	192.168.2.4	0xc6d8	No error (0)	workspacin.cloud		104.21.16.155	A (IP address)	IN (0x0001)	false
May 11, 2024 00:05:43.138046026 CEST	1.1.1.1	192.168.2.4	0xc6d8	No error (0)	workspacin.cloud		172.67.213.171	A (IP address)	IN (0x0001)	false
May 11, 2024 00:06:01.079061031 CEST	1.1.1.1	192.168.2.4	0xc19b	No error (0)	uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io	pub-ingress-aws-euc1.cloud-ara.tyk.io		CNAME (Canonical name)	IN (0x0001)	false
May 11, 2024 00:06:01.079061031 CEST	1.1.1.1	192.168.2.4	0xc19b	No error (0)	pub-ingress-aws-euc1.cloud-ara.tyk.io	ae1f8849daaac4ee6b80681872ab88b9-1762121307.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false

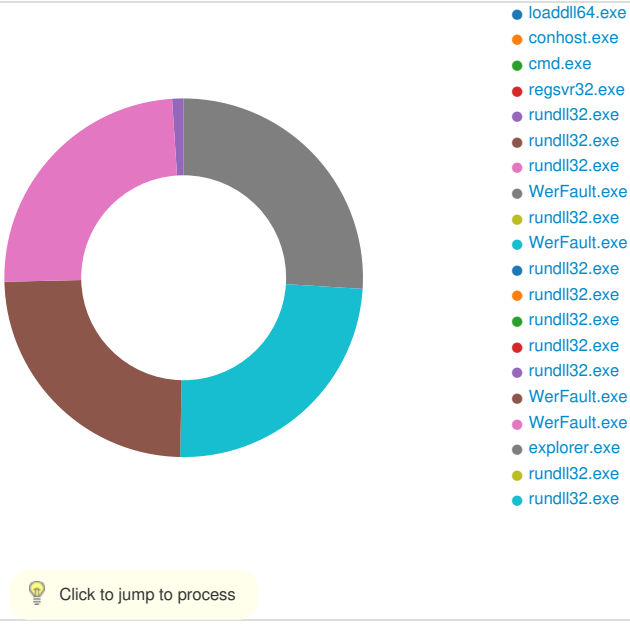
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 11, 2024 00:06:01.079061031 CEST	1.1.1.1	192.168.2.4	0xc19b	No error (0)	ae1f8849daaac4ee6b80681872ab88b9-1762121307.eu-central-1.elb.amazonaws.com		3.69.236.35	A (IP address)	IN (0x0001)	false
May 11, 2024 00:06:01.079061031 CEST	1.1.1.1	192.168.2.4	0xc19b	No error (0)	ae1f8849daaac4ee6b80681872ab88b9-1762121307.eu-central-1.elb.amazonaws.com		35.157.36.116	A (IP address)	IN (0x0001)	false
May 11, 2024 00:06:01.079061031 CEST	1.1.1.1	192.168.2.4	0xc19b	No error (0)	ae1f8849daaac4ee6b80681872ab88b9-1762121307.eu-central-1.elb.amazonaws.com		3.72.42.242	A (IP address)	IN (0x0001)	false
May 11, 2024 00:06:08.864455938 CEST	1.1.1.1	192.168.2.4	0x7f64	No error (0)	ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io	pub-ingress-aws-use1.cloud-ara.tyk.io		CNAME (Canonical name)	IN (0x0001)	false
May 11, 2024 00:06:08.864455938 CEST	1.1.1.1	192.168.2.4	0x7f64	No error (0)	pub-ingress-aws-use1.cloud-ara.tyk.io	ae97372e4f96e4d1299fbaeb7130b656-1584023256.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
May 11, 2024 00:06:08.864455938 CEST	1.1.1.1	192.168.2.4	0x7f64	No error (0)	ae97372e4f96e4d1299fbaeb7130b656-1584023256.us-east-1.elb.amazonaws.com		54.175.181.104	A (IP address)	IN (0x0001)	false
May 11, 2024 00:06:08.864455938 CEST	1.1.1.1	192.168.2.4	0x7f64	No error (0)	ae97372e4f96e4d1299fbaeb7130b656-1584023256.us-east-1.elb.amazonaws.com		54.159.36.188	A (IP address)	IN (0x0001)	false
May 11, 2024 00:06:08.864455938 CEST	1.1.1.1	192.168.2.4	0x7f64	No error (0)	ae97372e4f96e4d1299fbaeb7130b656-1584023256.us-east-1.elb.amazonaws.com		35.172.8.165	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- boriz400.com
- altynbe.com
- ridiculous-breakpoint-gw.aws-use1.cloud-ara.tyk.io
- anikvan.com
- uncertain-kitten-gw.aws-euc1.cloud-ara.tyk.io
- workspacin.cloud

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: **6632**, Parent PID: **2580**

General

Target ID:	0
Start time:	00:03:58
Start date:	11/05/2024
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\upfilles.dll.dll"
Imagebase:	0x7ff61d400000
File size:	165'888 bytes
MD5 hash:	763455F9DCB24DFEECC2B9D9F8D46D52
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

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: conhost.exe PID: **6636**, Parent PID: **6632**

General

Target ID:	1
Start time:	00:03:59
Start date:	11/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 344, Parent PID: 6632

General

Target ID:	2
Start time:	00:03:59
Start date:	11/05/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\upfilles.dll.dll",#1
Imagebase:	0x7ff70e6c0000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

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: regsvr32.exe PID: 2180, Parent PID: 6632

General

Target ID:	3
Start time:	00:03:59
Start date:	11/05/2024
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /i /s C:\Users\user\Desktop\upfilles.dll.dll
Imagebase:	0x7ff64ee30000
File size:	25'088 bytes
MD5 hash:	B0C2FA35D14A9FAD919E99D9D75E1B9E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: rundll32.exe PID: **5472**, Parent PID: **344**

General	
Target ID:	4
Start time:	00:03:59
Start date:	11/05/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\upfilles.dll.dll",#1
Imagebase:	0x7ff74e4b0000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: rundll32.exe PID: **6296**, Parent PID: **6632**

General	
Target ID:	5
Start time:	00:03:59
Start date:	11/05/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\upfilles.dll.dll,DllCanUnloadNow
Imagebase:	0x7ff74e4b0000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: rundll32.exe PID: **6324**, Parent PID: **6632**

General	
Target ID:	6
Start time:	00:04:02
Start date:	11/05/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\upfilles.dll.dll,DllGetClassObject
Imagebase:	0x7ff74e4b0000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: WerFault.exe PID: **6688**, Parent PID: **6324**

General

Target ID:	9
Start time:	00:04:02
Start date:	11/05/2024
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6324 -s 344
Imagebase:	0x7ff67a3b0000
File size:	570'736 bytes
MD5 hash:	FD27D9F6D02763BDE32511B5DF7FF7A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\2435a4f4-12e8-4f12-b3d3-a2af8ffc9df1	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\5781d2f1-eef3-4f47-ab07-5c6c3b9817e2	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\f83c447c-12d4-4692-8818-5c56d4f3a042	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\c9fcbf54-30c8-40f2-abbd-2a4763f68983	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E1D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E1D.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\d93b8e8c-9b61-4c9e-ad60-9ea39ba9b904	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_dc8a9dd96bb43aa654aa29aa9f464ac6a31131f_9db0ef65_8641b0ad-46f6-452c-a496-10d58d4ec871	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_dc8a9dd96bb43aa654aa29aa9f464ac6a31131f_9db0ef65_8641b0ad-46f6-452c-a496-10d58d4ec871\dcc937db-6e05-4a0a-976c-2b20c8d9fb4c	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_dc8a9dd96bb43aa654aa29aa9f464ac6a31131f_9db0ef65_8641b0ad-46f6-452c-a496-10d58d4ec871\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	0	32	4d 44 4d 50 fd fd 61 fd 0e 00 00 00 20 00 00 00 00 00 00 00 99 3e 66 fd 05 12 00 00 00 00 00	MDMPa >f	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	5128	6	00 00 00 00 00 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	200	1420	09 00 06 00 08 fd 04 01 0a 00 00 00 00 00 00 00 65 4a 00 00 02 00 00 00 08 14 00 00 00 01 00 00 4c 77 fd 10 fd 03 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 54 05 00 00 fd 03 00 00 fd 18 00 00 99 3e 66 00 00 00 00 00 00 00 00 fd 07 00 00 fd 07 00 00 fd 07 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 75 00 6d 00 6d 00 65 00 72 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00	eJLwT>f0W. Europe Standard TimeW. Europe Summer Time	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	5784	1232	fd 0b 56 1b fd 01 00 00 fd fd 21 fd 7f 00 00 fd 55 02 fd 01 00 00 00 00 00 01 00 00 00 00 00 fd fd 31 fd fd 00 00 00 fd 6e 2c 1d fd 7f 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 02 02 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 00 00 00 00 6f fd fd fd 00 00 00 00 fd 6d 03 fd 01 00 00 00 58 58 02 fd 01 00 00 00 fd 55 02 fd 01 00 00 00 fd fd 31 fd fd 00 00 00 00 00 4b 4e fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 6d 03 fd 01 00 00 00 3e 04 04 00 00 00 00 00 0c 16 00 30 00 00 00 00 fd fd fd fd fd fd fd fd 61 2d 1b fd 01 00 00 0a 00 00 00 00 00 00 00 62 62 2d 1b fd 01 00 00 fd 26 2e 1b fd 01 00 00 b0 00 fd 01 00 00	V!U1n,_3++S++omXXU1 KNm>0a-bb-&.	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	1620	168	fd 18 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 b0 00 fd 01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 04 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 04 00 00 fd 16 00 00	>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	11944	20	12 00 00 00 5a fd 00 fd 01 00 00 00 00 01 00 00 fd 2f 00 00	Z/	success or wait	18	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	12236	256	fd fd fd fd fd 40 55 41 56 48 fd fd 38 48 fd 05 fd fd 02 00 48 33 fd 48 fd 44 24 28 4d fd fd 48 fd fd 4c fd fd 4d fd fd 75 0a fd 03 40 00 fd fd 14 01 00 00 48 fd 74 24 68 33 fd 49 fd 30 39 35 fd fd 02 00 75 0a fd fd fd 00 fd fd fd 00 00 00 48 fd 0d 7e fd 02 00 4c fd 05 7f fd 02 00 48 fd 5c 24 50 49 3b fd 0f fd fd 00 00 00 48 fd 19 48 fd fd 74 2b 48 39 73 10 74 25 48 fd 13 fd 02 41 39 01 75 1b fd 42 04 41 39 41 04 75 12 fd 42 08 41 39 41 08 75 09 fd 42 0c 41 39 41 0c 74 0e 48 fd fd 08 49 3b fd 72 fd fd 00 00 00 48 fd 7c 24 30 48 fd 7b 20 48 fd 0f 48 fd fd 75 53 48 fd 0d 20 fd 02 00 fd 15 fd fd 01 00 48 39 37 75 2c 48 fd 4b 18 4c fd 44 24 20 48 fd 15 fd fd 01 00 48 fd 74 24 20 fd 53 10 fd fd fd fd 78 0e 48 fd 4c 24 20 fd 15 54 fd 01 00 48 fd 07 48 fd	@UAVH8HH3HD$(MHLMu@Ht$h3I095uH ~LH\$PI;HHt+H9st%HA9uBA9AuBA9AuBA9AtHI;rH|$0H{HHuSH H97u,HKLD$HHt$ SxHL$ THH	success or wait	17	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	51660	9064	fd fd fd 1f fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 55 fd fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	pUH	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	1788	4	04 00 00 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	7016	1232	fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 31 fd fd 00 00 00 fd fd fd fd fd fd fd fd fd fd 31 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 31 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 fd 20 22 fd 7f 00	3++S++F111T "	success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	1936	48	30 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 55 fd fd 00 00 00 fd fd 6f fd fd 00 00 00 28 04 00 00 fd 30 00 00 fd 04 00 00 fd 29 00 00	0 Uo(0)	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	1996	4	17 00 00 00		success or wait	23	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	5134	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	23	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	4376	752	00 00 01 22 fd 7f 00 00 00 50 11 00 7d 30 12 00 fd 13 09 37 fd 16 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 fd 07 61 4a 00 00 0a 00 fd 07 61 4a 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 0d fd 0f 00 02 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 02 00 00 00 00 00 60 fd 02 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 24 58 05 00 00 00 00 00 27 fd 05 00 00 00 00 00 00 00 00 00 00 00 00 00 72 fd 19 00 00 00 00 00 fd 10 06 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 33 06 00 00 00 00	"P}07aJaJ?"`AZb`$X'r@3	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	60724	5346	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 00 00 00 00 01 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 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49	EventEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketI	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D40.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 09 00 00 fd 07 00 00 05 00 00 00 24 01 00 00 fd 2e 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 0d 00 00 1e fd 00 00 15 00 00 00 fd 01 00 00 fd 11 00 00 16 00 00 00 fd 00 00 00 70 13 00 00	$.T8Tp	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 39 00 30 00 34 00 35 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>19045</Build>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	478	138	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 39 00 30 00 34 00 31 00 2e 00 32 00 30 00 30 00 36 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 76 00 62 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 39 00 31 00 32 00 30 00 36 00 2d 00 31 00 34 00 30 00 36 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>19041.2006.amd64fre.vb_release.191206-1406</BuildString>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	616	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	620	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	624	50	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 32 00 30 00 30 00 36 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>2006</Revision>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	674	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	678	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	682	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	754	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	758	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	762	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	826	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	830	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	834	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 32 00 30 00 35 00 37 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>2057</LCID>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	868	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	872	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	874	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	920	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	924	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	926	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	966	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	970	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	974	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6324</Pid>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1004	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1008	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1012	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 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>rundll32.exe</ImageName>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1082	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1086	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1090	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1180	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1184	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1188	40	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 37 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>479</Uptime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1228	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1232	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1236	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.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	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1436	96	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 32 00 32 00 30 00 33 00 34 00 30 00 38 00 31 00 37 00 39 00 32 00 30 00 30 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>2203408179200</PeakVirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1532	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1536	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1542	80	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 32 00 32 00 30 00 33 00 34 00 30 00 38 00 31 00 37 00 31 00 30 00 30 00 38 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>2203408171008</VirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1622	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1626	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1632	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 38 00 33 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>1838</PageFaultCount>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1706	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1710	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1716	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 32 00 30 00 38 00 39 00 36 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>7208960</PeakWorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1822	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 32 00 30 00 34 00 38 00 36 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>72048 64</WorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	1912	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 30 00 36 00 34 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 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	<QuotaPeakPagedPoolU sage>10646 4</QuotaPeakPagedPool Usage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2036	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 30 00 36 00 32 00 36 00 34 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 >106264</Q uotaPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2144	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 38 00 30 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedP oolUsage>18 088</QuotaPeakNonPag edPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2278	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 37 00 38 00 31 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>17816</QuotaNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2396	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 34 00 36 00 32 00 32 00 37 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1462272</PagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2482	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 34 00 37 00 30 00 34 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1470464</PeakPagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2574	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2578	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2584	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 34 00 36 00 32 00 32 00 37 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1462272</PrivateUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2656	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2660	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2664	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2710	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2714	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2718	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2748	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2752	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2758	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2798	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2802	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2810	30	3c 00 50 00 69 00 64 00 3e 00 36 00 36 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6632</Pid>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2840	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2844	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2852	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 36 00 34 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>loaddll64.exe</ImageName>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2924	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2928	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	2936	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000 00000</Cm dLineSignature>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3026	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3030	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3038	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 36 00 33 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>3630</Uptime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3080	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3084	2	09 00		success or wait	4	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3092	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3182	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3246	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3304	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 33 00 34 00 39 00 38 00 30 00 38 00 36 00 34 00 30 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>4349808640</PeakVirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3394	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3398	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3408	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 33 00 34 00 35 00 37 00 30 00 34 00 34 00 34 00 38 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>4345704448</VirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3482	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3486	2	09 00		success or wait	5	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3496	72	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 39 00 34 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>941</PageFaultCount>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3568	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3572	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3582	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 33 00 34 00 39 00 37 00 39 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3497984</PeakWorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3678	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3682	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3692	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 33 00 33 00 37 00 39 00 32 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>3379200</WorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3772	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3776	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3786	112	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 37 00 34 00 35 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>74528</QuotaPeakPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3898	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3902	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	3912	96	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 36 00 36 00 35 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>66512</QuotaPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4008	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4012	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4022	122	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 34 00 37 00 38 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>4784</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4158	106	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 34 00 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>4208</QuotaNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4278	74	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 36 00 34 00 37 00 31 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>647168</PagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4352	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4356	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4366	90	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 36 00 35 00 39 00 34 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>659456</PeakPagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4456	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4460	2	09 00		success or wait	5	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4470	70	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 36 00 34 00 37 00 31 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>647168</PrivateUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4540	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4544	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4552	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4598	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4602	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4608	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4650	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4654	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4658	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4690	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4694	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4696	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4738	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4742	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4744	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4782	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4786	2	09 00		success or wait	2	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4790	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4852	4	0d 00 0a 00		success or wait	8	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4856	2	09 00		success or wait	16	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	4860	108	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 5f 00 75 00 70 00 66 00 69 00 6c 00 6c 00 65 00 73 00 2e 00 64 00 6c 00 6c 00 2e 00 64 00 6c 00 6c 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>rundll32.exe_upfiles.dll.dll</Parameter0>	success or wait	8	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	5542	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	5546	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	5548	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	5588	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	5592	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	5594	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	5632	4	0d 00 0a 00		success or wait	6	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	5636	2	09 00		success or wait	12	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	5640	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 39 00 30 00 34 00 35 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>10.0.19045.2.0.0.256.48</Parameter1>	success or wait	6	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6194	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6198	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6200	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6240	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6244	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6246	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6284	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6288	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6292	94	3c 00 4d 00 49 00 44 00 3e 00 39 00 32 00 43 00 38 00 36 00 46 00 37 00 43 00 2d 00 44 00 42 00 32 00 42 00 2d 00 34 00 46 00 36 00 41 00 2d 00 39 00 35 00 41 00 44 00 2d 00 39 00 38 00 42 00 34 00 41 00 32 00 41 00 45 00 30 00 30 00 38 00 41 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>92C86F7C-DB2B-4F6A-95AD-98B4A2AE008A</MID>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6386	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6390	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6394	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 70 00 74 00 68 00 77 00 67 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>bpthwg, Inc.</SystemManufacturer>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6500	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6504	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6508	98	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 62 00 70 00 74 00 68 00 77 00 67 00 32 00 30 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>bpthwg20,1</SystemProductName>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6606	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6610	2	09 00		success or wait	2	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6614	122	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 32 00 30 00 31 00 2e 00 30 00 30 00 56 00 2e 00 32 00 30 00 38 00 32 00 39 00 32 00 32 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 32 00 31 00 31 00 32 00 31 00 31 00 38 00 34 00 32 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>VMW201.00V.20829224.B64.2211211842</BIOSVersion>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6736	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6740	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6744	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 36 00 35 00 31 00 37 00 33 00 39 00 39 00 39 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1665173999</OSInstallDate>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6826	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6830	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6834	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 32 00 33 00 2d 00 31 00 30 00 2d 00 30 00 33 00 54 00 30 00 38 00 3a 00 35 00 37 00 3a 00 31 00 38 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>2023-10-03T08:57:18Z</OSInstallTime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6936	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6940	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	6944	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7014	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7018	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7060	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7064	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.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</UEFI SecureBootEnabled>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7204	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7208	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7246	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7250	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7276	4	0d 00 0a 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7280	2	09 00		success or wait	6	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.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 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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7528	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7532	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7534	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7560	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7564	2	09 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7566	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 34 00 2d 00 30 00 35 00 2d 00 31 00 30 00 54 00 32 00 32 00 3a 00 30 00 34 00 3a 00 30 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2024-05-10T22:04:02Z">	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7666	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7670	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7674	254	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 33 00 32 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 35 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 31 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22 00 3e 00	<Process AsId="406" PID="6324" UptimeMS="15" TimeSinceCreationMS="15" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1">	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7928	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7932	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	7938	178	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 34 00 34 00 39 00 33 00 33 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="4493312" TimelineUnitShift="12" Timeline="1"/>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8116	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8120	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8124	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8144	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8148	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8150	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8188	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8192	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8194	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8232	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8236	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8240	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 36 00 34 00 31 00 62 00 30 00 61 00 64 00 2d 00 34 00 36 00 66 00 36 00 2d 00 34 00 35 00 32 00 63 00 2d 00 61 00 34 00 39 00 36 00 2d 00 31 00 30 00 64 00 35 00 38 00 64 00 34 00 65 00 63 00 38 00 37 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>8641b0ad-46f6-452c-a496-10d58d4ec871</Guid>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8338	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8342	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8346	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 34 00 2d 00 30 00 35 00 2d 00 31 00 30 00 54 00 32 00 32 00 3a 00 30 00 34 00 3a 00 30 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2024-05-10T22:04:02Z</CreationTime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8444	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8448	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8450	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8490	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DFD.tmp.WERInternalMetadata.xml	8494	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E1D.tmp.xml	0	4777	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_dc8a9dd96bb43aa654aa29aa9f464ac6a31131f_9db0ef65_8641b0ad-46f6-452c-a496-10d58d4ec871\Report.wer	0	2	fd fd		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_dc8a9dd96bb43aa654aa29aa9f464ac6a31131f_9db0ef65_8641b0ad-46f6-452c-a496-10d58d4ec871\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	150	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_dc8a9dd96bb43aa654aa29aa9f464ac6a31131f_9db0ef65_8641b0ad-46f6-452c-a496-10d58d4ec871\Report.wer	9388	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 38 00 37 00 32 00 34 00 31 00 38 00 31 00 37 00 32 00	MetadataHash=-872418172	success or wait	1	7FFE0E4D168F	unknown

Registry Activities

Analysis Process: rundll32.exe PID: 6516, Parent PID: 6632

General

Target ID:	10
Start time:	00:04:05
Start date:	11/05/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\upfilles.dll.dll,DllInstall
Imagebase:	0x7ff74e4b0000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Has exited:	true

Analysis Process: WerFault.exe PID: **3732**, Parent PID: **6516**

General

Target ID:	12
Start time:	00:04:05
Start date:	11/05/2024
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6516 -s 344
Imagebase:	0x7ff67a3b0000
File size:	570'736 bytes
MD5 hash:	FD27D9F6D02763BDE32511B5DF7FF7A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\33f89112-abef-46d4-9409-70ac392ee0d5	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\c351c02f-24e7-49f1-998e-7936ca155f26	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\ef76fe77-5310-444c-b4b5-d5a9b63c8504	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\f14db89c-95a6-41bc-b502-1125fc77d2ea	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3919.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3919.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\2d7ac2bf-94bc-4d12-92c9-64d8d9a9dc9a	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_964e80f5d1a5f925558a7e6299462efecb949df_9db0ef65_d9b8934c-437b-450d-af46-0185962b24b1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFE0E4D168F	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_964e80f5d1a5f925558a7e6299462efecb949df_9db0ef65_d9b8934c-437b-450d-af46-0185962b24b1\3a1839e8-8269-4126-b6b0-1e7d9a9f3b0b	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_964e80f5d1a5f925558a7e6299462efecb949df_9db0ef65_d9b8934c-437b-450d-af46-0185962b24b1\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	0	32	4d 44 4d 50 fd fd 61 fd 0e 00 00 00 20 00 00 00 00 00 00 59 3e 66 fd 05 12 00 00 00 00 00	MDMPa >f	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	5080	6	00 00 00 00 00 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	200	1420	09 00 06 00 08 fd 04 01 0a 00 00 00 00 00 00 00 65 4a 00 00 02 00 00 00 fd 13 00 00 00 01 00 00 4c 77 fd 10 fd 03 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 54 05 00 00 fd 03 00 00 74 19 00 00 59 3e 66 00 00 00 00 00 00 00 00 fd 07 00 00 fd 07 00 00 fd 07 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 75 00 6d 00 6d 00 65 00 72 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	eJLwTt>f0W. Europe Standard TimeW. Europe Summer Time	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	5736	1232	5f fd 58 fd 00 00 fd 0b 6c 16 25 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 53 fd 7b 00 00 00 20 04 03 00 00 00 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 47 02 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 00 00 00 00 00 00 50 fd 00 fd 01 00 00 00 20 04 03 00 00 00 00 00 00 00 4b 4e fd 7f 00 00 00 00 00 00 00 00 00 00 fd fd 53 7b 00 00 00 fd fd 53 fd 7b 00 00 00 20 04 03 00 00 00 00 00 00 00 00 00 00 00 00 00 34 62 fd 14 25 02 00 00 0a 00 00 00 00 00 00 00 6a 16 00 30 00 00 00 00 fd fd fd fd fd fd fd fd 61 fd 14 25 02 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 27 fd 14 25 02 00 00 50 fd 00 fd 01 00 00	Xl%S{ _3++S++GP KNS{S{ 4b%j0a%'%P	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	1620	168	fd 19 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 50 fd 00 fd 01 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 20 04 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 68 16 00 00	P h	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	10664	20	0e 00 00 00 32 00 fd 01 00 00 00 00 01 00 00 fd 2a 00 00	*	success or wait	14	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	10892	256	24 40 fd 09 05 00 00 48 fd fd fd 04 48 fd 5d 6f fd 42 31 0e 00 48 fd fd fd fd 05 00 00 fd fd 57 0d 00 48 fd fd 48 fd fd 48 fd 45 6f fd fd 05 00 00 fd fd fd 34 00 48 fd fd 48 fd 45 fd fd fd 05 00 00 33 7a 00 2e 04 00 44 fd 49 04 41 fd 00 30 00 00 48 fd 45 7f fd fd 0f fd 4d fd 0f fd 55 fd 0f fd fd 49 fd 00 10 04 fd 01 00 00 00 49 fd 01 10 04 fd 01 00 00 00 6b fd 16 48 fd 02 10 04 fd 01 00 00 00 48 fd 03 10 04 fd 01 00 00 00 48 fd 04 10 04 fd 01 00 00 00 4c 2b fd 4c 2b fd 48 2b fd 48 2b fd 4c 63 fd 4c fd fd 41 fd 02 00 00 00 4c fd fd 41 fd 00 fd 00 00 48 2b fd 49 fd 15 fd 47 fd 7a 14 fd 47 66 0f 1f fd 00 00 00 00 00 41 fd 47 fd 4d fd 49 05 48 63 fd 49 fd fd 48 fd fd 48 fd fd 48 2b fd 48 fd fd 48 03 fd 48 fd fd 04 48 6b fd 19 48 2b fd 49 2b fd 0f fd 44 0c	$@HH]oB1HWHHHEo4HHE3.DIA0HEMUIIkHHHL+L+H+H+LcLALAH+IGzGfAGMIHcIHHH+HHHHkH+I+D	success or wait	13	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	50436	2408	17 2e 1c 22 fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 5b fd 7b 00 00 00 fd fd 5b fd 7b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 20 71 fd 7b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 10 4b fd 14 25 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 2f fd 14 25 02 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6c 00 00 00 00 00 00 00 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	."[{{{ q{K%h/%ll	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	1788	4	03 00 00 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	6968	1232	fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 53 fd 7b 00 00 00 fd fd fd fd fd fd fd fd fd 53 fd 7b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 53 fd 7b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 fd 20 22 fd 7f 00	3++S++FS{S{S{T "	success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	1888	48	4c 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 70 71 fd 7b 00 00 00 fd fd 7b 00 00 00 68 0b 00 00 fd 2d 00 00 fd 04 00 00 fd 24 00 00	L pq{{h-$	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	1948	4	17 00 00 00		success or wait	23	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	5086	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	23	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	4328	752	00 00 01 22 fd 7f 00 00 00 50 11 00 7d 30 12 00 fd 13 09 37 50 16 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 fd 07 61 4a 00 00 0a 00 fd 07 61 4a 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 0d fd 0f 00 02 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 50 fd 02 00 00 00 00 00 60 fd 02 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 59 59 05 00 00 00 00 00 27 fd 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 31 fd 19 00 00 00 00 00 0f 1e 06 00 00 00 00 00 40 fd 1f 00 00 00 00 00 28 76 06 00 00 00 00	"P}07PaJaJ?"`AZbP`YY'1@(v	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	52844	5346	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 00 00 00 00 01 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 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49	EventEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketI	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER389A.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 09 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 0d 00 00 56 fd 00 00 15 00 00 00 fd 01 00 00 54 11 00 00 16 00 00 00 fd 00 00 00 40 13 00 00	)T8TVT@	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 39 00 30 00 34 00 35 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>19045</Build>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	478	138	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 39 00 30 00 34 00 31 00 2e 00 32 00 30 00 30 00 36 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 76 00 62 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 39 00 31 00 32 00 30 00 36 00 2d 00 31 00 34 00 30 00 36 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>19041.2006.amd64fre.vb_release.191206-1406</BuildString>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	616	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	620	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	624	50	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 32 00 30 00 30 00 36 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>2006</Revision>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	674	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	678	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	682	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	754	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	758	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	762	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	826	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	830	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	834	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 32 00 30 00 35 00 37 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>2057</LCID>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	868	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	872	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	874	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	920	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	924	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	926	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	966	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	970	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	974	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6516</Pid>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1004	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1008	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1012	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 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>rundll32.exe</ImageName>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1082	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1086	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1090	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000000</CmdLineSignature>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1180	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1184	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1188	40	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 34 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>245</Uptime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1228	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1232	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1236	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1436	96	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 32 00 32 00 30 00 33 00 34 00 30 00 37 00 36 00 35 00 34 00 39 00 31 00 32 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>2203407654912 </PeakVirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1532	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1536	2	09 00		success or wait	3	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1542	80	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 32 00 32 00 30 00 33 00 34 00 30 00 37 00 36 00 34 00 36 00 37 00 32 00 30 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>2203407646720</VirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1622	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1626	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1632	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 38 00 33 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>1832</PageFaultCount>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1706	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1710	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1716	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 31 00 38 00 34 00 33 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7184384</PeakWorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1822	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 31 00 38 00 30 00 32 00 38 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7180288</WorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	1912	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 30 00 36 00 34 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 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>106464</QuotaPeakPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2036	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 30 00 36 00 32 00 36 00 34 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>106264</QuotaPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2144	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 37 00 38 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>17888</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2278	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 37 00 36 00 31 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>17616</QuotaNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2396	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 33 00 38 00 34 00 34 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1384448</PagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2482	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 33 00 39 00 32 00 36 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1392640</PeakPagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2574	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2578	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2584	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 33 00 38 00 34 00 34 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1384448</PrivateUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2656	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2660	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2664	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2710	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2714	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2718	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2748	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2752	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2758	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2798	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2802	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2810	30	3c 00 50 00 69 00 64 00 3e 00 36 00 36 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6632</Pid>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2840	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2844	2	09 00		success or wait	4	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2852	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 36 00 34 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>loaddll64.exe</ImageName>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2924	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2928	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	2936	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>000000</CmdLineSignature>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3026	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3030	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3038	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 34 00 31 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6412</Uptime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3080	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3084	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3092	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3182	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3246	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	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3304	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 33 00 34 00 39 00 38 00 30 00 38 00 36 00 34 00 30 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>4349808640</PeakVirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3394	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3398	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3408	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 33 00 34 00 35 00 37 00 30 00 34 00 34 00 34 00 34 00 38 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>4345704448</VirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3482	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3486	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3496	72	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 39 00 34 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>941</PageFaultCount>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3568	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3572	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3582	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 33 00 34 00 39 00 37 00 39 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3497984</PeakWorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3678	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3682	2	09 00		success or wait	5	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3692	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 33 00 33 00 37 00 39 00 32 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>3379200</WorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3772	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3776	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3786	112	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 37 00 34 00 35 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>74528</QuotaPeakPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3898	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3902	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	3912	96	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 36 00 36 00 35 00 31 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	<QuotaPagedPoolUsage>66512</QuotaPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4008	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4012	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4022	122	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 34 00 37 00 38 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>4784</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4158	106	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 34 00 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>4208</QuotaNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4264	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4278	74	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 36 00 34 00 37 00 31 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>647168</PagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4352	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4356	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4366	90	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 36 00 35 00 39 00 34 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>659456</PeakPagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4456	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4460	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4470	70	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 36 00 34 00 37 00 31 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>647168</PrivateUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4540	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4544	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4552	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4598	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4602	2	09 00		success or wait	3	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4608	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4650	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4654	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4658	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4690	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4694	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4696	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4738	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4742	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4744	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4782	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4786	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4790	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4852	4	0d 00 0a 00		success or wait	8	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4856	2	09 00		success or wait	16	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	4860	108	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 5f 00 75 00 70 00 66 00 69 00 6c 00 6c 00 65 00 73 00 2e 00 64 00 6c 00 6c 00 2e 00 64 00 6c 00 6c 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>rundll32.exe_upfiles.dll.dll</Parameter0>	success or wait	8	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	5542	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	5546	2	09 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	5548	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	5588	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	5592	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	5594	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	5632	4	0d 00 0a 00		success or wait	6	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	5636	2	09 00		success or wait	12	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	5640	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 39 00 30 00 34 00 35 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>10.0.19045.2.0.0.256.48</Parameter1>	success or wait	6	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6194	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6198	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6200	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6240	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6244	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6246	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6284	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6288	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6292	94	3c 00 4d 00 49 00 44 00 3e 00 39 00 32 00 43 00 38 00 36 00 46 00 37 00 43 00 2d 00 44 00 42 00 32 00 42 00 2d 00 34 00 46 00 36 00 41 00 2d 00 39 00 35 00 41 00 44 00 2d 00 39 00 38 00 42 00 34 00 41 00 32 00 41 00 45 00 30 00 30 00 38 00 41 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>92C86F7C-DB2B-4F6A-95AD-98B4A2AE008A</MID>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6386	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6390	2	09 00		success or wait	2	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6394	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 70 00 74 00 68 00 77 00 67 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>bpthwg, Inc.</SystemManufacturer>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6500	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6504	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6508	98	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 62 00 70 00 74 00 68 00 77 00 67 00 32 00 30 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>bpthwg20,1</SystemProductName>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6606	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6610	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6614	122	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 32 00 30 00 31 00 2e 00 30 00 30 00 56 00 2e 00 32 00 30 00 38 00 32 00 39 00 32 00 32 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 32 00 31 00 31 00 32 00 31 00 31 00 38 00 34 00 32 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>VMW201.00V.20829224.B64.2211211842</BIOSVersion>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6736	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6740	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6744	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 36 00 35 00 31 00 37 00 33 00 39 00 39 00 39 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1665173999</OSInstallDate>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6826	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6830	2	09 00		success or wait	2	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6834	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 32 00 33 00 2d 00 31 00 30 00 2d 00 30 00 33 00 54 00 30 00 38 00 3a 00 35 00 37 00 3a 00 31 00 38 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>2023-10-03T08:57:18Z</OSInstallTime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6936	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6940	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	6944	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7014	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7018	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7060	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7064	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.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</UEFI SecureBootEnabled>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7204	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7208	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.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	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7246	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7250	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7276	4	0d 00 0a 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7280	2	09 00		success or wait	6	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.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 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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7528	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7532	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7534	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7560	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7564	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7566	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 34 00 2d 00 30 00 35 00 2d 00 31 00 30 00 54 00 32 00 32 00 3a 00 30 00 34 00 3a 00 30 00 35 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2024-05-10T22:04:05Z">	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7666	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7670	2	09 00		success or wait	2	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7674	254	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 31 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 35 00 31 00 36 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 31 00 35 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 31 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22 00 3e 00	<Process AsId="411" PID="6516" UptimeMS="15" TimeSinceCreationMS="15" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1">	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7928	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7932	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	7938	178	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 34 00 34 00 39 00 33 00 33 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="4493312" TimelineUnitShift="12" Timeline="1"/>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8116	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8120	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8124	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8144	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8148	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8150	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	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8188	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8192	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8194	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8232	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8236	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8240	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 39 00 62 00 38 00 39 00 33 00 34 00 63 00 2d 00 34 00 33 00 37 00 62 00 2d 00 34 00 35 00 30 00 64 00 2d 00 61 00 66 00 34 00 36 00 2d 00 30 00 31 00 38 00 35 00 39 00 36 00 32 00 62 00 32 00 34 00 62 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>d9b8934c-437b-450d-af46-0185962b24b1</Guid>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8338	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8342	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8346	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 34 00 2d 00 30 00 35 00 2d 00 31 00 30 00 54 00 32 00 32 00 3a 00 30 00 34 00 3a 00 30 00 35 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2024-05-10T22:04:05Z</CreationTime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8444	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8448	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8450	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8490	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38DA.tmp.WERInternalMetadata.xml	8494	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	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3919.tmp.xml	0	4777	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 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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_964e80f5d1a5f925558a7e6299462efecb949df_9db0ef65_d9b8934c-437b-450d-af46-0185962b24b1\Report.wer	0	2	fd fd		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_964e80f5d1a5f925558a7e6299462efecb949df_9db0ef65_d9b8934c-437b-450d-af46-0185962b24b1\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	150	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_964e80f5d1a5f925558a7e6299462efecb949df_9db0ef65_d9b8934c-437b-450d-af46-0185962b24b1\Report.wer	9388	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 32 00 34 00 31 00 37 00 33 00 39 00 37 00 35 00 32 00	MetadataHash=241739752	success or wait	1	7FFE0E4D168F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0f1f9877-fe5f-9883-d9d5-aa88f27dc06d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{0f1f9877-fe5f-9883-d9d5-aa88f27dc06d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{0f1f9877-fe5f-9883-d9d5-aa88f27dc06d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFE0E4D0D97	unknown

Analysis Process: rundll32.exe PID: **7264**, Parent PID: **6632**

General

Target ID:	13
Start time:	00:04:08
Start date:	11/05/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\upfilles.dll.dll",DllCanUnloadNow
Imagebase:	0x7ff74e4b0000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: rundll32.exe PID: **7272**, Parent PID: **6632**

General	
Target ID:	14
Start time:	00:04:08
Start date:	11/05/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\upfilles.dll.dll",DllGetClassObject
Imagebase:	0x7ff74e4b0000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: rundll32.exe PID: **7288**, Parent PID: **6632**

General	
Target ID:	15
Start time:	00:04:08
Start date:	11/05/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\upfilles.dll.dll",DllInstall
Imagebase:	0x7ff74e4b0000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: rundll32.exe PID: **7296**, Parent PID: **6632**

General	
Target ID:	16
Start time:	00:04:08
Start date:	11/05/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\upfilles.dll.dll",DllUnregisterServer
Imagebase:	0x7ff74e4b0000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

File Activities						
There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.						
File Path	**Offset**	**Length**	**Completion**	**Count**	**Source Address**	**Symbol**

Analysis Process: rundll32.exe PID: **7320**, Parent PID: **6632**

General	
Target ID:	18
Start time:	00:04:08
Start date:	11/05/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\upfilles.dll.dll",stow
Imagebase:	0x7ff74e4b0000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.2415718994.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.1868997096.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.2680109233.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.1843049394.0000029213423000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Latrodectus, Description: Yara detected Latrodectus, Source: 00000012.00000003.1867725723.00000292135D0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000002.2938154508.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.2762031046.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Latrodectus, Description: Yara detected Latrodectus, Source: 00000012.00000003.1868887059.00000292135D1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Latrodectus, Description: Yara detected Latrodectus, Source: 00000012.00000003.1868680221.00000292135D0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.2797091473.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.1843192476.0000029213423000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.2311970800.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.2397236802.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Latrodectus, Description: Yara detected Latrodectus, Source: 00000012.00000003.1867965215.00000292135D0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.2810418995.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.2001079033.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Latrodectus, Description: Yara detected Latrodectus, Source: 00000012.00000003.1867247710.00007DF4F0220000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.2738453835.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.2284307888.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.2738816096.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Bazar_2, Description: Yara detected Bazar Loader, Source: 00000012.00000002.2938671459.0000029211650000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Bazar_2, Description: Yara detected Bazar Loader, Source: 00000012.00000002.2938735431.00000292116A0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.1842909028.0000029213422000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.2311847302.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.1882552320.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.2284190577.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.2042061481.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Latrodectus, Description: Yara detected Latrodectus, Source: 00000012.00000003.1868287262.00000292135D0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.1991839967.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Latrodectus, Description: Yara detected Latrodectus, Source: 00000012.00000003.1868470583.00000292135D0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BruteRatel_1, Description: Yara detected BruteRatel, Source: 00000012.00000003.1867444760.000002921161C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Has exited:	false

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	292130179DC	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	292130179DC	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	292130179DC	HttpSendRequestA

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	292130179DC	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	292130179DC	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	292130179DC	HttpSendRequestA
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	292130179DC	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	292130179DC	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	292130179DC	HttpSendRequestA
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	292130179DC	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	292130179DC	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	292130179DC	HttpSendRequestA

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Update	unicode	rundll32 "C:\Users\user\AppData\Roaming\upfilles.dll", stow...`.U.`.....#..p..8.. `.....	success or wait	1	7DF4F02B016D	RegSetValueExW

Analysis Process: WerFault.exe PID: **7388**, Parent PID: **7272**

General

Target ID:	20
Start time:	00:04:08
Start date:	11/05/2024
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 7272 -s 344

Imagebase:	0x7ff67a3b0000
File size:	570'736 bytes
MD5 hash:	FD27D9F6D02763BDE32511B5DF7FF7A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\ba3bc84f-5946-4680-ae1d-65b528dbde9d	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\863fe75f-6033-4e27-b20a-b17dfe7c951b	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\765330b5-35e2-477b-b0fc-6916c3ea2537	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\d840b9a1-fc23-475b-b0a6-34afba621993	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4648.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4648.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\a623fc17-f158-47d6-970b-e2105c9cac02	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_dc8a9dd96bb43aa654aa29aa9f464ac6a31131f_9db0ef65_7dc7f057-dc81-4d91-9caa-bd8701d223a3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_dc8a9dd96bb43aa654aa29aa9f464ac6a31131f_9db0ef65_7dc7f057-dc81-4d91-9caa-bd8701d223a3\d94f0c4f-0ec2-487b-b55d-b65f85616e06	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_dc8a9dd96bb43aa654aa29aa9f464ac6a31131f_9db0ef65_7dc7f057-dc81-4d91-9caa-bd8701d223a3\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	0	32	4d 44 4d 50 fd fd 61 fd 0e 00 00 00 20 00 00 00 00 00 00 00 19 3e 66 fd 05 12 00 00 00 00 00	MDMPa >f	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	5080	6	00 00 00 00 00 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	200	1420	09 00 06 00 08 fd 04 01 0a 00 00 00 00 00 00 00 65 4a 00 00 02 00 00 00 fd 13 00 00 00 01 00 00 4c 77 fd 10 fd 03 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 54 05 00 00 fd 03 00 00 68 1c 00 00 19 3e 66 00 00 00 00 00 00 00 00 fd 07 00 00 fd 07 00 00 fd 07 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 75 00 6d 00 6d 00 65 00 72 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	eJLwTh>f0W. Europe Standard TimeW. Europe Summer Time	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	5736	1232	01 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 fd 55 02 fd 01 00 00 00 fd 6e 2c 1d fd 7f 00 00 03 00 00 00 00 00 00 00 fd 2c 1d fd 7f 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 02 02 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 00 00 00 00 00 00 00 6f fd fd fd 00 00 00 00 fd 6d 03 fd 01 00 00 00 58 58 02 fd 01 00 00 00 fd 55 02 fd 01 00 00 00 fd fd fd 6c 00 00 00 00 00 4b 4e fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 6d 03 fd 01 00 00 00 46 04 02 00 00 00 00 00 0c 16 00 30 00 00 00 00 fd fd fd fd fd fd fd fd 5c 46 42 fd 01 00 00 0a 00 00 00 00 00 00 00 66 5d 46 42 fd 01 00 00 38 18 47 42 fd 01 00 00 b0 00 fd 01 00 00	Un,,_3++S++omXXUlKN mF0\FBf]FB8GB	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	1620	168	6c 1c 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 b0 00 fd 01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 46 04 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 04 00 00 68 16 00 00	lFh	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	10664	20	0f 00 00 00 5a fd 00 fd 01 00 00 00 00 01 00 00 fd 2a 00 00	Z*	success or wait	15	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	10908	256	fd fd fd fd fd fd 40 55 41 56 48 fd fd 38 48 fd 05 fd fd 02 00 48 33 fd 48 fd 44 24 28 4d fd fd 48 fd fd 4c fd fd 4d fd fd 75 0a fd 03 40 00 fd fd 14 01 00 00 48 fd 74 24 68 33 fd 49 fd 30 39 35 fd fd 02 00 75 0a fd fd fd 00 fd fd fd 00 00 00 48 fd 0d 7e fd 02 00 4c fd 05 7f fd 02 00 48 fd 5c 24 50 49 3b fd 0f fd fd 00 00 00 48 fd 19 48 fd fd 74 2b 48 39 73 10 74 25 48 fd 13 fd 02 41 39 01 75 1b fd 42 04 41 39 41 04 75 12 fd 42 08 41 39 41 08 75 09 fd 42 0c 41 39 41 0c 74 0e 48 fd fd 08 49 3b fd 72 fd fd 00 00 00 48 fd 7c 24 30 48 fd 7b 20 48 fd 0f 48 fd fd 75 53 48 fd 0d 20 fd 02 00 fd 15 fd fd 01 00 48 39 37 75 2c 48 fd 4b 18 4c fd 44 24 20 48 fd 15 fd fd 01 00 48 fd 74 24 20 fd 53 10 fd fd fd fd 78 0e 48 fd 4c 24 20 fd 15 54 fd 01 00 48 fd 07 48 fd	@UAVH8HH3HD$(MHLMu@Ht$h3I095uH~LH\$PI;HHt+H9st%HA9uBA9AuBA9AuBA9AtHI;rH|$0H{HHuSH H97u,HKLD$HHt$ SxHL$ THH	success or wait	14	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	42636	9512	fd fd fd 1f fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 7f 6c 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 48 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	IH	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	1788	4	03 00 00 00		success or wait	3	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	6968	1232	fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 6c 00 00 00 fd fd fd fd fd fd fd fd fd fd 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 fd 20 22 fd 7f 00	3++S++FlllT "	success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	1888	48	fd 1c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 7f 6c 00 00 00 38 fd fd fd 6c 00 00 00 fd 05 00 00 20 00 00 fd 04 00 00 fd 24 00 00	l8l$	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	1948	4	17 00 00 00		success or wait	23	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	5086	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	23	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	4328	752	00 00 01 22 fd 7f 00 00 00 50 11 00 7d 30 12 00 fd 13 09 37 50 16 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 fd 07 61 4a 00 00 0a 00 fd 07 61 4a 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 0d fd 0f 00 02 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 40 fd 02 00 00 00 00 00 60 fd 02 00 00 00 00 79 fd 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fd 5a 05 00 00 00 00 00 27 fd 05 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 00 00 00 00 41 3e 06 00 00 00 00 00 40 fd 1f 00 00 00 00 00 28 76 06 00 00 00 00	"P}07PaJaJ?"`AZb@`yZ'A>@(v	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	52148	5346	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 00 00 00 00 01 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 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49	EventEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketI	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER459B.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 09 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 0d 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 54 11 00 00 16 00 00 00 fd 00 00 00 40 13 00 00	)T8TT@	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 39 00 30 00 34 00 35 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>19045</Build>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	478	138	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 39 00 30 00 34 00 31 00 2e 00 32 00 30 00 30 00 36 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 76 00 62 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 39 00 31 00 32 00 30 00 36 00 2d 00 31 00 34 00 30 00 36 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>19041.2006.amd64fre.vb_release.191206-1406</BuildString>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	616	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	620	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	624	50	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 32 00 30 00 30 00 36 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>2006</Revision>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	674	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	678	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	682	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	754	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	758	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	762	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	826	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	830	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	834	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 32 00 30 00 35 00 37 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>2057</LCID>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	868	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	872	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	874	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	920	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	924	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	926	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	966	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	970	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	974	30	3c 00 50 00 69 00 64 00 3e 00 37 00 32 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7272</Pid>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1004	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1008	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1012	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 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>rundll32.exe</ImageName>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1082	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1086	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1090	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1180	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1184	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1188	40	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 31 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>617</Uptime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1228	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1232	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1236	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.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	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1436	96	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 32 00 32 00 30 00 33 00 34 00 30 00 37 00 36 00 35 00 34 00 39 00 31 00 32 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>2203407654912</PeakVirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1532	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1536	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1542	80	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 32 00 32 00 30 00 33 00 34 00 30 00 37 00 36 00 34 00 36 00 37 00 32 00 30 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>2203407646720</VirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1622	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1626	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1632	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 38 00 33 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1831</PageFaultCount>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1706	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1710	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1716	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 31 00 39 00 32 00 35 00 37 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>7192576</PeakWorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1822	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 31 00 38 00 38 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7188480</WorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	1912	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 30 00 36 00 34 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 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>106464</QuotaPeakPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2036	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 30 00 36 00 32 00 36 00 34 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>106264</QuotaPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2144	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 37 00 36 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>17696</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2278	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 37 00 34 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>17424</QuotaNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2396	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 33 00 37 00 36 00 32 00 35 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>1376256</PagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2482	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 33 00 38 00 34 00 34 00 34 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>1384448</PeakPagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2574	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2578	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2584	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 33 00 37 00 36 00 32 00 35 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>1376256</PrivateUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2656	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2660	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2664	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2710	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2714	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2718	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2748	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2752	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2758	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2798	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2802	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2810	30	3c 00 50 00 69 00 64 00 3e 00 36 00 36 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6632</Pid>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2840	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2844	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2852	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 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>(unable to retrieve)</ImageName>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2938	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2942	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	2950	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 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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3040	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3044	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3052	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 38 00 31 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>9812</Uptime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3094	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3098	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3106	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3184	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3188	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3196	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3248	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3252	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3260	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3304	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3308	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3318	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 33 00 38 00 33 00 31 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>4383166464</PeakVirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3408	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3412	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3422	56	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 30 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>0</VirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3478	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3482	2	09 00		success or wait	5	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3492	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 37 00 36 00 34 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>1764</PageFaultCount>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3566	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3570	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3580	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 36 00 30 00 37 00 38 00 34 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>6078464</PeakWorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3676	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3680	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3690	76	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 33 00 32 00 37 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>32768</WorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3780	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 32 00 33 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>142336</QuotaPeakPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3894	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3898	2	09 00		success or wait	5	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3908	90	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 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>96</QuotaPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	3998	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4002	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4012	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>7736</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4134	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4138	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4148	106	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 32 00 31 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>1216</QuotaNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4254	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4258	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4268	72	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 37 00 37 00 38 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>77824</PagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4340	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4344	2	09 00		success or wait	5	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4354	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 31 00 37 00 35 00 35 00 35 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>1175552</PeakPagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4446	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4450	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4460	68	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 37 00 37 00 38 00 32 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>77824</PrivateUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4528	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4532	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4540	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4586	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4590	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4596	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4638	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4642	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4646	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4678	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4682	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4684	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4726	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4730	2	09 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4732	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4770	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4774	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4778	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4840	4	0d 00 0a 00		success or wait	8	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4844	2	09 00		success or wait	16	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	4848	108	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 5f 00 75 00 70 00 66 00 69 00 6c 00 6c 00 65 00 73 00 2e 00 64 00 6c 00 6c 00 6c 00 2e 00 64 00 6c 00 6c 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>rundll32.exe_upfiles.dll.dll</Parameter0>	success or wait	8	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	5530	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	5534	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	5536	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	5576	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	5580	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	5582	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	5620	4	0d 00 0a 00		success or wait	6	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	5624	2	09 00		success or wait	12	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	5628	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 39 00 30 00 34 00 35 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>10.0.19045.2.0.0.256.48</Parameter1>	success or wait	6	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6182	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6186	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6188	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6228	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6232	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6234	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6272	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6276	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6280	94	3c 00 4d 00 49 00 44 00 3e 00 39 00 32 00 43 00 38 00 36 00 46 00 37 00 43 00 2d 00 44 00 42 00 32 00 42 00 2d 00 34 00 46 00 36 00 41 00 2d 00 39 00 35 00 41 00 44 00 2d 00 39 00 38 00 42 00 34 00 41 00 32 00 41 00 45 00 30 00 30 00 38 00 41 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>92C86F7C-DB2B-4F6A-95AD-98B4A2AE008A</MID>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6374	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6378	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6382	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 62 00 70 00 74 00 68 00 77 00 67 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>bpthwg, Inc.</SystemManufacturer>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6488	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6492	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6496	98	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 62 00 70 00 74 00 68 00 77 00 67 00 32 00 30 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>bpthwg20,1</SystemProductName>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6594	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6598	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6602	122	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 32 00 30 00 31 00 2e 00 30 00 30 00 56 00 2e 00 32 00 30 00 38 00 32 00 39 00 32 00 32 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 32 00 31 00 31 00 32 00 31 00 31 00 38 00 34 00 32 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>VMW201.00V.20829224.B64.2211211842</BIOSVersion>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6724	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6728	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6732	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 36 00 35 00 31 00 37 00 33 00 39 00 39 00 39 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1665173999</OSInstallDate>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6814	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6818	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6822	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 32 00 33 00 2d 00 31 00 30 00 2d 00 30 00 33 00 54 00 30 00 38 00 3a 00 35 00 37 00 3a 00 31 00 38 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>2023-10-03T08:57:18Z</OSInstallTime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6924	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6928	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	6932	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7002	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7006	2	09 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7008	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7048	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7052	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7054	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7088	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7092	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7096	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7192	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7196	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7198	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7234	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7238	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7240	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7264	4	0d 00 0a 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7268	2	09 00		success or wait	6	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7272	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7516	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7520	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7522	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7548	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7552	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7554	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 34 00 2d 00 30 00 35 00 2d 00 31 00 30 00 54 00 32 00 32 00 3a 00 30 00 34 00 3a 00 30 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2024-05-10T22:04:08Z">	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7654	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7658	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7662	254	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 31 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 32 00 37 00 32 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 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22 00 3e 00	<Process AsId="416" PID="7272" UptimeMS="46" TimeSinceCreationMS="46" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1">	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7916	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7920	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	7926	178	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 34 00 34 00 39 00 37 00 34 00 30 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="4497408" TimelineUnitShift="12" Timeline="1"/>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8104	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8108	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8112	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8132	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8136	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8138	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8176	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8180	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8182	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8220	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8224	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8228	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 64 00 63 00 37 00 66 00 30 00 35 00 37 00 2d 00 64 00 63 00 38 00 31 00 2d 00 34 00 64 00 39 00 31 00 2d 00 39 00 63 00 61 00 61 00 2d 00 62 00 64 00 38 00 37 00 30 00 31 00 64 00 32 00 32 00 33 00 61 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>7dc7f057-dc81-4d91-9caa-bd8701d223a3</Guid>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8326	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8330	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8334	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 34 00 2d 00 30 00 35 00 2d 00 31 00 30 00 54 00 32 00 32 00 3a 00 30 00 34 00 3a 00 30 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2024-05-10T22:04:08Z</CreationTime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8432	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8436	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8438	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	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8478	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4619.tmp.WERInternalMetadata.xml	8482	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4648.tmp.xml	0	4777	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_dc8a9dd96bb43aa654aa29aa9f464ac6a31131f_9db0ef65_7dc7f057-dc81-4d91-9caa-bd8701d223a3\Report.wer	0	2	fd fd		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_dc8a9dd96bb43aa654aa29aa9f464ac6a31131f_9db0ef65_7dc7f057-dc81-4d91-9caa-bd8701d223a3\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	150	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_dc8a9dd96bb43aa654aa29aa9f464ac6a31131f_9db0ef65_7dc7f057-dc81-4d91-9caa-bd8701d223a3\Report.wer	9388	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 32 00 39 00 33 00 38 00 32 00 36 00 37 00 36 00 31 00	MetadataHash=293826761	success or wait	1	7FFE0E4D168F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0f1f9877-fe5f-9883-d9d5-aa88f27dc06d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{0f1f9877-fe5f-9883-d9d5-aa88f27dc06d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{0f1f9877-fe5f-9883-d9d5-aa88f27dc06d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFE0E4D0D97	unknown

Analysis Process: WerFault.exe PID: 7396, Parent PID: 7288

General

Target ID:	21
Start time:	00:04:08
Start date:	11/05/2024

Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 7288 -s 344
Imagebase:	0x7ff67a3b0000
File size:	570'736 bytes
MD5 hash:	FD27D9F6D02763BDE32511B5DF7FF7A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\bf1a83a1-4fe0-4214-acb7-e0b3d20b9acc	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\6b4ca3d3-0f12-44a5-b633-a35cf07a4d28	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\4a1c20ce-2f71-4bf5-b48c-f57cb9248e9b	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\546ec6ea-bf7e-45f6-a0d1-2f7c28ce5d9a	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4704.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4704.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\54367f61-6562-471d-900f-93ba349ae8c6	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_964e80f5d1a5f925558a7e6299462efecb949df_9db0ef65_6fb130ca-cac1-4736-bec2-e227247d8b1e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_964e80f5d1a5f925558a7e6299462efecb949df_9db0ef65_6fb130ca-cac1-4736-bec2-e227247d8b1e\c00f458f-d02b-4a8d-a270-57fc175f3cc8	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_upf_964e80f5d1a5f925558a7e6299462efecb949df_9db0ef65_6fb130ca-cac1-4736-bec2-e227247d8b1e\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	0	32	4d 44 4d 50 fd fd 61 fd 0e 00 00 00 20 00 00 00 00 00 00 00 19 3e 66 fd 05 12 00 00 00 00 00	MDMPa >f	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	5080	6	00 00 00 00 00 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	200	1420	09 00 06 00 08 fd 04 01 0a 00 00 00 00 00 00 00 65 4a 00 00 02 00 00 00 fd 13 00 00 00 01 00 00 4c 77 fd 10 fd 03 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 54 05 00 00 fd 03 00 00 78 1c 00 00 19 3e 66 00 00 00 00 00 00 00 00 fd 07 00 00 fd 07 00 00 fd 07 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 75 00 6d 00 6d 00 65 00 72 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	eJLwTx>f0W. Europe Standard TimeW. Europe Summer Time	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	5736	1232	30 fd 24 fd 00 00 00 44 04 04 00 00 00 00 00 00 00 00 00 00 00 00 00 30 fd 24 fd 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 47 02 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 00 00 00 00 00 00 00 00 50 fd 00 fd 01 00 00 00 44 04 04 00 00 00 00 00 00 00 4b 4e fd 7f 00 00 00 00 00 00 00 00 00 00 fd fd 24 fd 00 00 00 fd fd 24 fd 00 00 00 44 04 00 00 00 00 00 00 00 00 00 00 00 00 00 38 5d 5f 28 63 02 00 00 0a 00 00 00 00 00 00 00 6a 16 00 30 00 00 00 00 fd fd fd fd fd fd fd fd 5c 5f 28 63 02 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 0f 60 28 63 02 00 00 50 fd 00 fd 01 00 00	0D0_3++S++GPDKND8] _(cj0_(c`(cP	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	1620	168	7c 1c 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 50 fd 00 fd 01 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 44 04 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 04 00 00 68 16 00 00	|PDh	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	10664	20	0e 00 00 00 32 00 fd 01 00 00 00 00 01 00 00 fd 2a 00 00	*	success or wait	14	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	10892	256	24 40 fd 09 05 00 00 48 fd fd fd 04 48 fd 5d 6f fd 42 31 0e 00 48 fd fd fd fd 05 00 00 fd fd 57 0d 00 48 fd fd 48 fd fd 48 fd 45 6f fd fd 05 00 00 fd fd fd 34 00 48 fd fd 48 fd 45 fd fd fd 05 00 00 33 7a 00 2e 04 00 44 fd 49 04 41 fd 00 30 00 00 48 fd 45 7f fd fd 0f fd 4d fd 0f fd 55 fd 0f fd fd 49 fd 00 10 04 fd 01 00 00 00 49 fd 01 10 04 fd 01 00 00 00 6b fd 16 48 fd 02 10 04 fd 01 00 00 00 48 fd 03 10 04 fd 01 00 00 00 48 fd 04 10 04 fd 01 00 00 00 4c 2b fd 4c 2b fd 48 2b fd 48 2b fd 4c 63 fd 4c fd fd 41 fd 02 00 00 00 4c fd fd 41 fd 00 fd 00 00 48 2b fd 49 fd 15 fd 47 fd 7a 14 fd 47 66 0f 1f fd 00 00 00 00 00 41 fd 47 fd 4d fd 49 05 48 63 fd 49 fd fd 48 fd fd 48 fd fd 48 2b fd 48 fd fd 48 03 fd 48 fd fd 04 48 6b fd 19 48 2b fd 49 2b fd 0f fd 44 0c	$@HH]oB1HWHHHEo4HHE3.DIA0HEMUIIkHHHL+L+H+H+LcLALAH+IGzGfAGMIHcIHHH+HHHHkH+I+D	success or wait	13	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	49540	8	fd fd 0f fd fd 00 00 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	1788	4	03 00 00 00		success or wait	3	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	6968	1232	fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 24 fd 00 00 00 fd fd fd fd fd fd fd fd fd 24 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 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 24 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 fd 20 22 fd 7f 00	3++S++FT "	success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	1888	48	fd 1c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 48 fd 0f fd fd 00 00 00 fd 04 00 00 54 fd 00 00 fd 04 00 00 fd 24 00 00	HT$	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	1948	4	17 00 00 00		success or wait	23	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	5086	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	23	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	4328	752	00 00 01 22 fd 7f 00 00 00 50 11 00 7d 30 12 00 fd 13 09 37 50 16 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 fd 07 61 4a 00 00 0a 00 fd 07 61 4a 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 0d fd 0f 00 02 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 60 fd 02 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 5b 05 00 00 00 00 00 27 fd 05 00 00 00 00 00 00 00 00 00 00 00 00 00 77 19 00 00 00 00 00 63 47 06 00 00 00 00 00 40 fd 1f 00 00 00 00 00 28 76 06 00 00 00 00	"P}07PaJaJ?"`AZb`['cG@(v	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	49548	5346	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 00 00 00 00 01 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 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49	EventEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketI	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4656.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 09 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 0d 00 00 76 fd 00 00 15 00 00 00 fd 01 00 00 54 11 00 00 16 00 00 00 fd 00 00 00 40 13 00 00	)T8TvT@	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 39 00 30 00 34 00 35 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>19045</Build>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	478	138	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 39 00 30 00 34 00 31 00 2e 00 32 00 30 00 30 00 36 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 76 00 62 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 39 00 31 00 32 00 30 00 36 00 2d 00 31 00 34 00 30 00 36 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>19041.2006.amd64fre.vb_release.191206-1406</BuildString>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	616	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	620	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	624	50	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 32 00 30 00 30 00 36 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>2006</Revision>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	674	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	678	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	682	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	754	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	758	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	762	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	826	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	830	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	834	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 32 00 30 00 35 00 37 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>2057</LCID>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	868	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	872	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	874	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	920	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	924	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	926	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	966	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	970	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	974	30	3c 00 50 00 69 00 64 00 3e 00 37 00 32 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7288</Pid>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1004	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1008	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1012	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 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>rundll32.exe</ImageName>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1082	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1086	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1090	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1180	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1184	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1188	40	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 36 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>761</Uptime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1228	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1232	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1236	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.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	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1436	96	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 32 00 32 00 30 00 33 00 34 00 30 00 37 00 36 00 35 00 34 00 39 00 31 00 32 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>2203407654912</PeakVirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1532	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1536	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1542	80	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 32 00 32 00 30 00 33 00 34 00 30 00 37 00 36 00 34 00 36 00 37 00 32 00 30 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>2203407646720</VirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1622	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1626	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1632	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 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>1835</PageFaultCount>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1706	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1710	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1716	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 32 00 30 00 30 00 37 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7200768</PeakWorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1822	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 31 00 39 00 36 00 36 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7196672</WorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	1912	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 30 00 36 00 34 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 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>106464</QuotaPeakPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2036	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 30 00 36 00 32 00 36 00 34 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>106264</QuotaPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2144	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 37 00 37 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 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>17728</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2278	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 37 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>17456</QuotaNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2396	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 33 00 38 00 30 00 33 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1380352</PagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2482	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 33 00 38 00 38 00 35 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1388544</PeakPagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2574	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2578	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2584	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 33 00 38 00 30 00 33 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1380352</PrivateUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2656	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2660	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2664	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2710	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2714	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2718	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2748	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2752	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2758	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2798	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2802	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2810	30	3c 00 50 00 69 00 64 00 3e 00 36 00 36 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6632</Pid>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2840	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2844	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2852	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 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>(unable to retrieve)</ImageName>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2938	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2942	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	2950	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3040	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3044	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3052	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 39 00 36 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>9963</Uptime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3094	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3098	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3106	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3184	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3188	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3196	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3248	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3252	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3260	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3304	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3308	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3318	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 33 00 38 00 33 00 31 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>4383166464</PeakVirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3408	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3412	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3422	56	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 30 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>0</VirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3478	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3482	2	09 00		success or wait	5	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3492	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 37 00 36 00 34 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>1764</PageFaultCount>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3566	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3570	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3580	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 36 00 30 00 37 00 38 00 34 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>6078464</PeakWorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3676	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3680	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3690	76	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 33 00 32 00 37 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>32768</WorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3780	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 32 00 33 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>142336</QuotaPeakPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3894	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3898	2	09 00		success or wait	5	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3908	90	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 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>96</QuotaPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	3998	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4002	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4012	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>7736</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4134	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4138	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4148	106	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 32 00 31 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>1216</QuotaNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4254	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4258	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4268	72	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 37 00 37 00 38 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>77824</PagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4340	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4344	2	09 00		success or wait	5	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4354	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 31 00 37 00 35 00 35 00 35 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>1175552</PeakPagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4446	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4450	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4460	68	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 37 00 37 00 38 00 32 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>77824</PrivateUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4528	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4532	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4540	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4586	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4590	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4596	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4638	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4642	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4646	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4678	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4682	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4684	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4726	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4730	2	09 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4732	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4770	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4774	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4778	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4840	4	0d 00 0a 00		success or wait	8	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4844	2	09 00		success or wait	16	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	4848	108	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 5f 00 75 00 70 00 66 00 69 00 6c 00 6c 00 65 00 73 00 2e 00 64 00 6c 00 6c 00 2e 00 64 00 6c 00 6c 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>rundll32.exe_upfiles.dll.dll</Parameter0>	success or wait	8	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	5530	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	5534	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	5536	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	5576	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	5580	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	5582	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	5620	4	0d 00 0a 00		success or wait	6	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	5624	2	09 00		success or wait	12	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	5628	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 39 00 30 00 34 00 35 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>10.0.19045.2.0.0.256.48</Parameter1>	success or wait	6	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6182	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6186	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6188	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6228	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6232	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6234	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6272	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6276	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6280	94	3c 00 4d 00 49 00 44 00 3e 00 39 00 32 00 43 00 38 00 36 00 46 00 37 00 43 00 2d 00 44 00 42 00 32 00 42 00 2d 00 34 00 46 00 36 00 41 00 2d 00 39 00 35 00 41 00 44 00 2d 00 39 00 38 00 42 00 34 00 41 00 32 00 41 00 45 00 30 00 30 00 38 00 41 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>92C86F7C-DB2B-4F6A-95AD-98B4A2AE008A</MID>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6374	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6378	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6382	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 62 00 70 00 74 00 68 00 77 00 67 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>bpthwg, Inc.</SystemManufacturer>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6488	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6492	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6496	98	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 62 00 70 00 74 00 68 00 77 00 67 00 32 00 30 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>bpthwg20,1</SystemProductName>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6594	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6598	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6602	122	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 32 00 30 00 31 00 2e 00 30 00 30 00 56 00 2e 00 32 00 30 00 38 00 32 00 39 00 32 00 32 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 32 00 31 00 31 00 32 00 31 00 31 00 38 00 34 00 32 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>VMW201.00V.20829224.B64.2211211842</BIOSVersion>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6724	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6728	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6732	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 36 00 35 00 31 00 37 00 33 00 39 00 39 00 39 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1665173999</OSInstallDate>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6814	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6818	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6822	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 32 00 33 00 2d 00 31 00 30 00 2d 00 30 00 33 00 54 00 30 00 38 00 3a 00 35 00 37 00 3a 00 31 00 38 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>2023-10-03T08:57:18Z</OSInstallTime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6924	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6928	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	6932	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7002	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7006	2	09 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7008	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7048	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7052	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7054	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7088	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7092	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7096	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7192	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7196	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7198	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7234	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7238	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7240	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7264	4	0d 00 0a 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7268	2	09 00		success or wait	6	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7272	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7516	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7520	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7522	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7548	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7552	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7554	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 34 00 2d 00 30 00 35 00 2d 00 31 00 30 00 54 00 32 00 32 00 3a 00 30 00 34 00 3a 00 30 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2024-05-10T22:04:08Z">	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7654	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7658	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7662	254	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 31 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 32 00 38 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22 00 3e 00	<Process AsId="417" PID="7288" UptimeMS="46" TimeSinceCreationMS="46" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1">	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7916	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7920	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	7926	178	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 34 00 34 00 39 00 37 00 34 00 30 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="4497408" TimelineUnitShift="12" Timeline="1"/>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8104	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8108	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8112	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8132	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8136	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8138	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8176	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8180	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8182	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8220	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8224	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8228	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 66 00 62 00 31 00 33 00 30 00 63 00 61 00 2d 00 63 00 61 00 63 00 31 00 2d 00 34 00 37 00 33 00 36 00 2d 00 62 00 65 00 63 00 32 00 2d 00 65 00 32 00 32 00 37 00 32 00 34 00 37 00 64 00 38 00 62 00 31 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>6fb130ca-cac1-4736-bec2-e227247d8b1e</Guid>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8326	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8330	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8334	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 34 00 2d 00 30 00 35 00 2d 00 31 00 30 00 54 00 32 00 32 00 3a 00 30 00 34 00 3a 00 30 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2024-05-10T22:04:08Z</CreationTime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8432	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8436	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8438	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	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8478	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46C4.tmp.WERInternalMetadata.xml	8482	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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4704.tmp.xml	0	4777	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 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	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E7A.tmp.txt	0	2	42 00	B	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E7A.tmp.txt	2	22	2e 00 54 00 69 00 6d 00 65 00 72 00 52 00 65 00 73 00 6f 00 6c 00	.TimerResol	success or wait	150	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E7A.tmp.txt	9388	46	35 00 35 00 0d 00 0a 00 50 00 2e 00 46 00 69 00 72 00 73 00 74 00 4c 00 65 00 76 00 65 00 6c 00 54 00 62 00 46 00 69 00 6c 00 6c 00 73 00	55P.FirstLevelTbFills	success or wait	1	7FFE0E4D168F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0f1f9877-fe5f-9883-d9d5-aa88f27dc06d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{0f1f9877-fe5f-9883-d9d5-aa88f27dc06d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{0f1f9877-fe5f-9883-d9d5-aa88f27dc06d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFE0E4D0D97	unknown

Analysis Process: explorer.exe PID: 2580, Parent PID: 7320

General

Target ID:	22
Start time:	00:04:16
Start date:	11/05/2024
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff72b770000

File size:	5'141'208 bytes
MD5 hash:	662F4F92FDE3557E86D110526BB578D5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Latrodectus, Description: Yara detected Latrodectus, Source: 00000016.00000003.2703639060.0000000003250000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Latrodectus, Description: Yara detected Latrodectus, Source: 00000016.00000000.1844669819.00000000013A0000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Latrodectus, Description: Yara detected Latrodectus, Source: 00000016.00000003.2807505534.0000000008820000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Latrodectus, Description: Yara detected Latrodectus, Source: 00000016.00000002.2945149697.000000000B52C000.00000004.00000010.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Latrodectus, Description: Yara detected Latrodectus, Source: 00000016.00000002.2938259956.0000000003140000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Latrodectus, Description: Yara detected Latrodectus, Source: 00000016.00000002.2937512886.00000000013A0000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security
Has exited:	false

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

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **7856**, Parent PID: **2580**

General

Target ID:	26
Start time:	00:04:29
Start date:	11/05/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\rundll32.exe" "C:\Users\user\AppData\Roaming\upfilles.dll", stow
Imagebase:	0x7ff74e4b0000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: rundll32.exe PID: **7984**, Parent PID: **2580**

General

Target ID:	27
Start time:	00:04:37
Start date:	11/05/2024

Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\rundll32.exe" "C:\Users\user\AppData\Roaming\upfilles.dll", stow
Imagebase:	0x7ff74e4b0000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Disassembly

No disassembly