ID: 346331
Sample Name: A8xYhQFvXo
Cookbook: default.jbs
Time: 14:22:06
Date: 30/01/2021
Version: 31.0.0 Emerald

Table of Contents

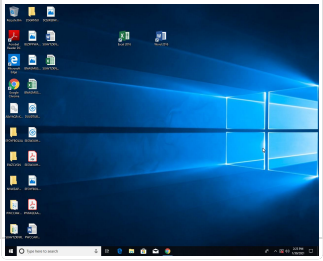
Analysis Report A8xYhQFvXo

Overview

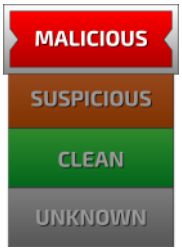
General Information

Sample Name:	A8xYhQFvXo (renamed file extension from none to dll)
Analysis ID:	346331
MD5:	83dd317c95f4acb..
SHA1:	04f9227cc3bfde5..
SHA256:	5b2f060f1512100..
Tags:	Mingloa

Most interesting Screenshot:



Detection

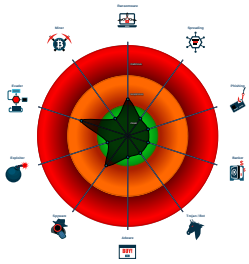


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Machine Learning detection for samp…
- Checks if the current process is bein…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to query locale…
- Contains functionality which may be…
- Detected potential crypto function
- One or more processes crash
- PE file contains executable resource…
- Sample execution stops while proce…
- Sample file is different than original

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6628 cmdline: loaddll32.exe 'C:\Users\user\Desktop\A8xYhQFvXo.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - rundll32.exe (PID: 6652 cmdline: rundll32.exe C:\Users\user\Desktop\A8xYhQFvXo.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6708 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6652 -s 712 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6896 cmdline: rundll32.exe C:\Users\user\Desktop\A8xYhQFvXo.dll,Hello002 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6972 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6896 -s 712 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7004 cmdline: rundll32.exe C:\Users\user\Desktop\A8xYhQFvXo.dll,Hello003 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7092 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7004 -s 712 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
A8xYhQFvXo.dll	APT34_PICKPOCKET	unknown	unknown	• 0x200c9c:$s2: \nss3.dll • 0x249d10:$s2: \nss3.dll • 0x3fc4f0:$s4: \| %Q \|\| substr(name,%d+18) ELSE name END WHERE tbl_name=%Q COLLATE nocase AND (type='table' OR type='index' OR type='trigger'); • 0x1d0d44:$s5: \Login Data • 0x1d0e34:$s5: \Login Data • 0x1d0f24:$s5: \Login Data • 0x1d1064:$s5: \Login Data • 0x1d1274:$s5: \Login Data • 0x1d12f4:$s5: \Login Data • 0x1d1374:$s5: \Login Data • 0x1d1438:$s5: \Login Data • 0x1d1634:$s5: \Login Data • 0x1d1744:$s5: \Login Data • 0x1d18d4:$s5: \Login Data • 0x1d1944:$s5: \Login Data • 0x200d10:$s6: %s\Mozilla\Firefox\profiles.ini • 0x249d90:$s6: %s\Mozilla\Firefox\profiles.ini • 0x1d0d45:$s7: Login Data • 0x1d0e35:$s7: Login Data • 0x1d0f25:$s7: Login Data • 0x1d1065:$s7: Login Data

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.236067014.000000001028B000.00000008.00020000.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x1556d6:$xo1: /\x13\x12\x08[\x0B\x09\x14\x1C\x09\x1A\x16[\x18\x1A\x15\x15\x14\x0F[\x19\x1E[\x09\x0E\x15[\x12\x15[?4([\x16\x14\x1F\x1E
00000007.00000002.245505715.000000001028B000.00000008.00020000.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x1556d6:$xo1: /\x13\x12\x08[\x0B\x09\x14\x1C\x09\x1A\x16[\x18\x1A\x15\x15\x14\x0F[\x19\x1E[\x09\x0E\x15[\x12\x15[?4([\x16\x14\x1F\x1E
00000001.00000002.230780419.000000001028B000.00000008.00020000.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x1556d6:$xo1: /\x13\x12\x08[\x0B\x09\x14\x1C\x09\x1A\x16[\x18\x1A\x15\x15\x14\x0F[\x19\x1E[\x09\x0E\x15[\x12\x15[?4([\x16\x14\x1F\x1E

Unpacked PEs

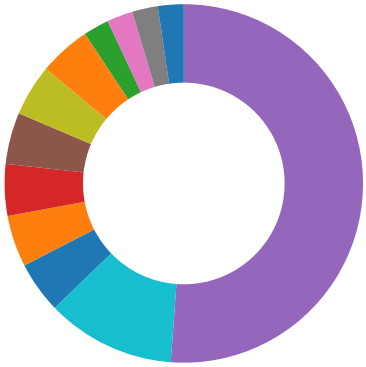
Source	Rule	Description	Author	Strings
1.2.rundll32.exe.10000000.1.unpack	APT34_PICKPOCKET	unknown	unknown	• 0x200c9c:$s2: \nss3.dll • 0x249d10:$s2: \nss3.dll • 0x3fc4f0:$s4: \| %Q \|\| substr(name,%d+18) ELSE name END WHERE tbl_name=%Q COLLATE nocase AND (type='table' OR type='index' OR type='trigger'); • 0x1d0d44:$s5: \Login Data • 0x1d0e34:$s5: \Login Data • 0x1d0f24:$s5: \Login Data • 0x1d1064:$s5: \Login Data • 0x1d1274:$s5: \Login Data • 0x1d12f4:$s5: \Login Data • 0x1d1374:$s5: \Login Data • 0x1d1438:$s5: \Login Data • 0x1d1634:$s5: \Login Data • 0x1d1744:$s5: \Login Data • 0x1d18d4:$s5: \Login Data • 0x1d1944:$s5: \Login Data • 0x200d10:$s6: %s\Mozilla\Firefox\profiles.ini • 0x249d90:$s6: %s\Mozilla\Firefox\profiles.ini • 0x1d0d45:$s7: Login Data • 0x1d0e35:$s7: Login Data • 0x1d0f25:$s7: Login Data • 0x1d1065:$s7: Login Data

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.10000000.1.unpack	APT34_PICKPOCKET	unknown	unknown	• 0x200c9c:$s2: \nss3.dll • 0x249d10:$s2: \nss3.dll • 0x3fc4f0:$s4: \| %Q \|\| substr(name,%d+18) ELSE name END WHERE tbl_name=%Q COLLATE nocase AND (type='table' OR type='index' OR type='trigger'); • 0x1d0d44:$s5: \Login Data • 0x1d0e34:$s5: \Login Data • 0x1d0f24:$s5: \Login Data • 0x1d1064:$s5: \Login Data • 0x1d1274:$s5: \Login Data • 0x1d12f4:$s5: \Login Data • 0x1d1374:$s5: \Login Data • 0x1d1438:$s5: \Login Data • 0x1d1634:$s5: \Login Data • 0x1d1744:$s5: \Login Data • 0x1d18d4:$s5: \Login Data • 0x1d1944:$s5: \Login Data • 0x200d10:$s6: %s\Mozilla\Firefox\profiles.ini • 0x249d90:$s6: %s\Mozilla\Firefox\profiles.ini • 0x1d0d45:$s7: Login Data • 0x1d0e35:$s7: Login Data • 0x1d0f25:$s7: Login Data • 0x1d1065:$s7: Login Data
7.2.rundll32.exe.10000000.1.unpack	APT34_PICKPOCKET	unknown	unknown	• 0x200c9c:$s2: \nss3.dll • 0x249d10:$s2: \nss3.dll • 0x3fc4f0:$s4: \| %Q \|\| substr(name,%d+18) ELSE name END WHERE tbl_name=%Q COLLATE nocase AND (type='table' OR type='index' OR type='trigger'); • 0x1d0d44:$s5: \Login Data • 0x1d0e34:$s5: \Login Data • 0x1d0f24:$s5: \Login Data • 0x1d1064:$s5: \Login Data • 0x1d1274:$s5: \Login Data • 0x1d12f4:$s5: \Login Data • 0x1d1374:$s5: \Login Data • 0x1d1438:$s5: \Login Data • 0x1d1634:$s5: \Login Data • 0x1d1744:$s5: \Login Data • 0x1d18d4:$s5: \Login Data • 0x1d1944:$s5: \Login Data • 0x200d10:$s6: %s\Mozilla\Firefox\profiles.ini • 0x249d90:$s6: %s\Mozilla\Firefox\profiles.ini • 0x1d0d45:$s7: Login Data • 0x1d0e35:$s7: Login Data • 0x1d0f25:$s7: Login Data • 0x1d1065:$s7: Login Data

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Binary contains paths to debug symbols

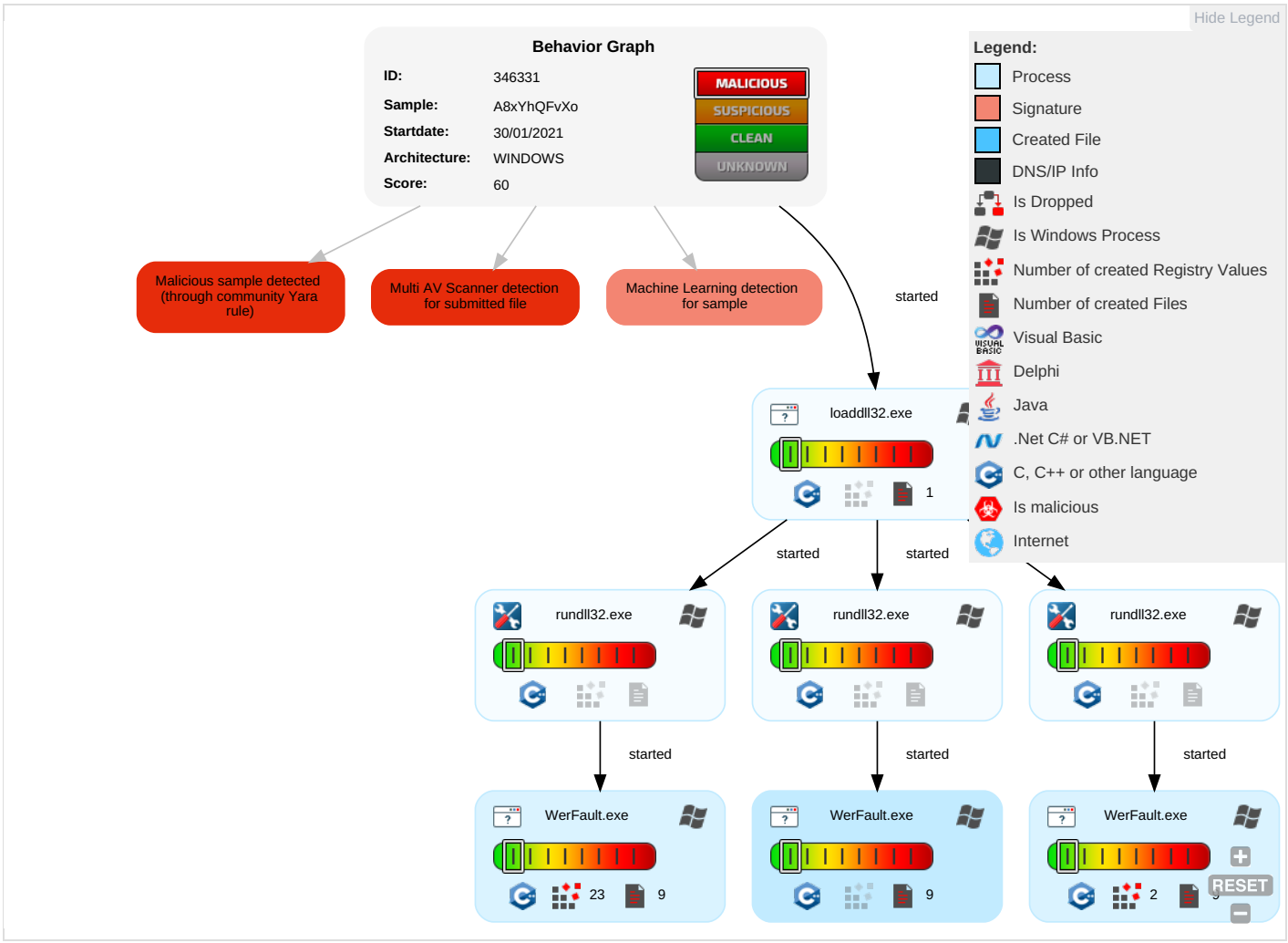
System Summary:

Malicious sample detected (through community Yara rule)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Rer Ser Effe
Valid Accounts	Native API 1	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Rer Tra Witl Aut
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rundll32 1	LSASS Memory	Security Software Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Rer Wip Witl Aut
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obt Dev Clo Bac
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

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
A8xYhQFvXo.dll	17%	Virustotal		Browse
A8xYhQFvXo.dll	19%	Metadefender		Browse
A8xYhQFvXo.dll	44%	ReversingLabs	Win32.Trojan.Mingloa	
A8xYhQFvXo.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://01%s08%s15%s22%sWebGL%d%02d%s.club/01%s08%s15%s22%sFrankLin%d%02d%s.xyz/post_info.	0%	Avira URL Cloud	safe	
http://https://twitter.comsec-fetch-dest:	0%	Avira URL Cloud	safe	
http://https://www.instagram.comsec-fetch-mode:	0%	Avira URL Cloud	safe	
http://https://twitter.comReferer:	0%	Avira URL Cloud	safe	
http://www.interestvideo.com/video1.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://01%s08%s15%s22%sWebGL%d%02d%s.club/01%s08%s15%s22%sFrankLin%d%02d%s.xyz/post_info.	rundll32.exe, 00000001.0000000 2.230693439.00000000101CE000.0 0000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000 000101CE000.00000002.00020000. sdmp, rundll32.exe, 00000007.0 0000002.245432696.00000000101C E000.00000002.00020000.sdmp, A 8xYhQFvXo.dll	false	• Avira URL Cloud: safe	low
http://https://upload.twitter.com/i/media/upload.jsoncommand=FINALIZE&media_id=	rundll32.exe, 00000001.0000000 2.230693439.00000000101CE000.0 0000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000 000101CE000.00000002.00020000. sdmp, rundll32.exe, 00000007.0 0000002.245432696.00000000101C E000.00000002.00020000.sdmp, A 8xYhQFvXo.dll	false		high
http://https://twitter.com/compose/tweetsec-fetch-dest:	rundll32.exe, 00000001.0000000 2.230693439.00000000101CE000.0 0000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000 000101CE000.00000002.00020000. sdmp, rundll32.exe, 00000007.0 0000002.245432696.00000000101C E000.00000002.00020000.sdmp, A 8xYhQFvXo.dll	false		high
http://https://www.instagram.com/	A8xYhQFvXo.dll	false		high
http://https://www.messenger.com/	rundll32.exe, 00000001.0000000 2.230693439.00000000101CE000.0 0000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000 000101CE000.00000002.00020000. sdmp, rundll32.exe, 00000007.0 0000002.245432696.00000000101C E000.00000002.00020000.sdmp, A 8xYhQFvXo.dll	false		high
http://https://upload.twitter.com/i/media/upload.json%dcommand=INIT&total_bytes=&media_type=image%2Fjpeg&me	rundll32.exe, 00000001.0000000 2.230693439.00000000101CE000.0 0000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000 000101CE000.00000002.00020000. sdmp, rundll32.exe, 00000007.0 0000002.245432696.00000000101C E000.00000002.00020000.sdmp, A 8xYhQFvXo.dll	false		high
http://https://upload.twitter.com/i/media/upload.json?command=APPEND&media_id=%s&segment_index=0accept:	rundll32.exe, 00000001.0000000 2.230693439.00000000101CE000.0 0000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000 000101CE000.00000002.00020000. sdmp, rundll32.exe, 00000007.0 0000002.245432696.00000000101C E000.00000002.00020000.sdmp, A 8xYhQFvXo.dll	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.twitter.com/1.1/statuses/update.jsoninclude_profile_interstitial_type=1&include_blocking	rundll32.exe, 00000001.00000002.230693439.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245432696.00000000101CE000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false		high
http://https://www.messenger.com/origin:	rundll32.exe, 00000001.00000002.230693439.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245432696.00000000101CE000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false		high
http://https://twitter.com/	rundll32.exe, 00000001.00000002.230693439.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245432696.00000000101CE000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false		high
http://https://twitter.com/ookie:	rundll32.exe, 00000001.00000002.230693439.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245432696.00000000101CE000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false		high
http://https://api.twitter.com/1.1/statuses/update.json	rundll32.exe, 00000001.00000002.230693439.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245432696.00000000101CE000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false		high
http://https://curl.haxx.se/docs/http-cookies.html	rundll32.exe, 00000001.00000002.230642928.0000000010171000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235936438.0000000010171000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245392829.0000000010171000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false		high
http://https://twitter.comsec-fetch-dest:	A8xYhQFvXo.dll	false	• Avira URL Cloud: safe	unknown
http://https://upload.twitter.com/i/media/upload.json	rundll32.exe, 00000001.00000002.230693439.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245432696.00000000101CE000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false		high
http://https://twitter.com/compose/tweetsec-fetch-mode:	A8xYhQFvXo.dll	false		high
http://https://www.instagram.comsec-fetch-mode:	rundll32.exe, 00000001.00000002.230693439.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245432696.00000000101CE000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/accounts/login/ajax/facebook/	A8xYhQFvXo.dll	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.instagram.com/sec-fetch-site:	rundll32.exe, 00000001.00000002.230693439.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245432696.00000000101CE000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false		high
http://https://twitter.comReferer:	A8xYhQFvXo.dll	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com/accept:	rundll32.exe, 00000001.00000002.230693439.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245432696.00000000101CE000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false		high
http://www.interestvideo.com/video1.php	A8xYhQFvXo.dll	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com	rundll32.exe, 00000001.00000002.230693439.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245432696.00000000101CE000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false		high
http://https://www.instagram.com/accept:	rundll32.exe, 00000001.00000002.230693439.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245432696.00000000101CE000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false		high
http://https://www.messenger.com/login/nonce/	rundll32.exe, 00000001.00000002.230693439.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245432696.00000000101CE000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false		high
http://https://www.messenger.com/login/nonce/ookie:	rundll32.exe, 00000001.00000002.230693439.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245432696.00000000101CE000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false		high
http://https://upload.twitter.com/i/media/upload.json?command=APPEND&media_id=%s&segment_index=0	rundll32.exe, 00000001.00000002.230693439.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000004.00000002.235972167.00000000101CE000.00000002.00020000.sdmp, rundll32.exe, 00000007.00000002.245432696.00000000101CE000.00000002.00020000.sdmp, A8xYhQFvXo.dll	false		high
http://https://www.instagram.com/graphql/query/?query_hash=149bef52a3b2af88c0fec37913fe1cbc&variables=%7B%2	A8xYhQFvXo.dll	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald

Analysis ID:	346331
Start date:	30.01.2021
Start time:	14:22:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	A8xYhQFvXo (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.winDLL@10/12@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 95.7%) • Quality average: 76.1% • Quality standard deviation: 26.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated
Warnings:	Show All • Exclude process from analysis (whitelisted): WerFault.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 13.88.21.125 • Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, skypedataprdcolwus15.cloudapp.net

Simulations

Behavior and APIs

Time	Type	Description
14:23:06	API Interceptor	3x Sleep call for process: WerFault.exe modified
14:23:11	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5a155b1e9b8901355626d9881b9ed599cf1223_82810a17_1b0352d0\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12526
Entropy (8bit):	3.771298130946976
Encrypted:	false
SSDEEP:	192:Reiq0oXAdHBUZMX4jed+qM/u7sUS274ltWc7:Ei8XiBUZMX4jey/u7sUX4ltWc7
MD5:	DF86840392878D8F23C871F2E70B796C
SHA1:	C7C4E2ACF2DCC505C36F65B27AC6295237FE230D
SHA-256:	C4C8476A732491F39F347BB3CF53FB7859E52E335DEB280B0E3381832744431F
SHA-512:	A2015F5D4DF264A4C5BD994E7AA8B0E23632E410F07F7804EC05A5F57EC431926ED69B6E794E53F88C4BF9CBEC423A88AC1570700953B6E169E6ACAD42C10D4F
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.6.5.1.8.9.8.7.1.9.7.1.4.0.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.6.5.1.8.9.8.8.5.8.7.7.6.8.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.e.6.a.9.8.9.6.-.1.5.6.6.-.4.a.c.5.-.9.9.8.2.-.b.3.d.9.7.e.d.a.e.e.1.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.0.1.7.d.0.8.3.-.2.8.e.6.-.4.b.5.c.-.8.d.d.2.-.8.e.7.8.f.1.2.e.8.5.3.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....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.a.f.0.-.0.0.0.1.-.0.0.1.7.-.b.8.d.d.-.b.c.7.a.5.6.f.7.d.6.0.1.....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.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_9155b230567b23dc90309f27732428df1d2d4b15_82810a17_1a0b4812\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12524
Entropy (8bit):	3.771244807080854
Encrypted:	false
SSDEEP:	192:s6i00oX0cHBUZMX4jed+qM/u7sUS274ltWcu:9iCXdBUZMX4jey/u7sUX4ltWcu
MD5:	A8BBCF85BFD93259DCA577CCBA62C6DF
SHA1:	130D348413E2ED000B1621AA9C2A3A0E80C8E559
SHA-256:	225C0218DF5763AD8275D5296449CCAB586476298EEA99B173609F90ADD1B05C
SHA-512:	937B31AFC1F835464D7A31251B051B77E493FF503C8D5A7819C30C4D95676E67C0DC04B76DB4E35534E3441F995A2D6317229CF075F40D28B71A76B0F13C3C70
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.6.5.1.8.9.8.4.2.9.0.8.9.9.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.6.5.1.8.9.8.5.3.3.7.7.7.7.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.4.9.0.0.c.7.7.-.9.b.3.2.-.4.f.c.d.-.a.2.a.3.-.d.0.6.7.4.3.b.a.2.e.3.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.2.e.f.6.a.8.4.-.c.d.4.d.-.4.9.d.f.-.b.8.b.5.-.3.a.d.e.4.b.f.d.8.7.1.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....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.f.c.-.0.0.0.1.-.0.0.1.7.-.d.a.5.9.-.c.5.7.8.5.6.f.7.d.6.0.1.....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.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_9155b230567b23dc90309f27732428df1d2d4b15_82810a17_1b8b63b8\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12522
Entropy (8bit):	3.7708356318523943
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_9155b230567b23dc90309f27732428df1d2d4b15_82810a17_1b8b63b8\Report.wer	
SSDEEP:	192:Geiy0oXMcHBUZMX4jed+qM/u7sUS274ItWcF:XiUXVBUZMX4jey/u7sUX4ItWcF
MD5:	192FD41F5E2D69E0D7466FA6DC55B573
SHA1:	6900AA02BA64E6BD4C83B288AFA06B8EB1B1F29A
SHA-256:	73475F8652413694AB066DD064A7CE658283399E8B15AB99DDE5EFDF1A4EA126
SHA-512:	9F399EB22247676DF72B14CED9E166DE4239BD197087FCE012CBE1357BE6F843BD9BBEBC3379B3BF30D48B5C58E02D2DFD2A4413344D247BB6C3FE13D969843
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.6.5.1.8.9.9.2.2.2.8.5.6.2.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.6.5.1.8.9.9.3.0.7.2.1.2.8.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.a.8.6.a.a.9.4.-.6.2.d.7.-.4.6.f.7.-.a.7.3.1.-.b.2.c.d.8.e.c.2.5.9.a.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.2.9.7.b.e.d.d.-.4.6.f.0.-.4.c.b.d.-.9.3.9.f.-.7.8.f.2.8.3.d.2.2.b.9.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....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.b.5.c.-.0.0.0.1.-.0.0.1.7.-.7.f.c.2.-.a.c.7.c.5.6.f.7.d.6.0.1.....T.a.r.g.e.t.A.p.p.l.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.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Jan 30 22:23:04 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	54380
Entropy (8bit):	2.0015561523103194
Encrypted:	false
SSDEEP:	192:nCduNZT6NASLzm9NbqLzdtQGd2K/WjZerJWGZKXZh4KzNxVw:CLzwbiCO27VeAGZOZhrRw
MD5:	9960CD95476181EF57DFC589CA17D6CE
SHA1:	13DB12E3C3A8645F2FD0D1EA6A45272C7FD689BC
SHA-256:	FBA058585194DA498260F97D7D25451379657E0BB3DDA7231050553EC44F8473
SHA-512:	2562F958B912B8B367417C90446C6B6F3F925710DC3B79D97CFFBDC44A1421612680CDF12E100DC787CE9420E24C6302C2796F88701F30A1C38A27B6149A0213
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....H..`.....U.....B.....D .....GenuineIntelW.....T.....E..`.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8266
Entropy (8bit):	3.6968442224830307
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiqT696YAT6Kh62mgmfTuSBCprRg89bNisfQvm:RrlsNie696Y06662mgmfTuSGdNhfl
MD5:	43BD54E768548B366930B31787D276A8
SHA1:	D5C19415165E51B494EAAD9DF4591D8EDB909D71
SHA-256:	335195883725319DA55D5CA8881958618530D96B6F0CE6CAAD6F82C44A658C95
SHA-512:	223D9237FC5DEC58112BFFCB7C646367A17B42E72708CFA0162F0137D61999929A30A3996950271577E0A1A5C800BFE4D0FF5055739455E8269B10A6A7B78A21
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.6.5.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER413E.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4629
Entropy (8bit):	4.472952170485334
Encrypted:	false
SSDEEP:	48:cvIwSD8zsxBJgtWI9G4WSC8BZ8fm8M4JCdsUFrX+q8/oJ34SrSCd:uITfVdxSNQJOX53DWCd
MD5:	779F5EA92B661C11A3A26AB103727370
SHA1:	366C7DDF4A32E5C0591C9E34849D9D6C4900BDC2

C:\ProgramData\Microsoft\Windows\WER\Temp\WER413E.tmp.xml	
SHA-256:	74D3C03945E2A0F8211980261729AC387EDD10FB56F6DDD5F5CA78B61FDF8EAF
SHA-512:	86C1FE4E3C75BA60CF81BEC9C5A0C409E25BC5F24FCC0FA6084D90CBD2D113BA3770E81A683C09B18874713A7DB4D3C391AEA284AF46E90F4F124412D9878B1
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="839973" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Jan 30 22:23:07 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	55552
Entropy (8bit):	1.962155911528806
Encrypted:	false
SSDEEP:	192:FciIrVXsfykKu65g9voRtOvi5QGd2K/WjZZdEyhZcw8InW:/w8fMuloRKvO27VZ2yhZ+IW
MD5:	C7014E8E5C3E4F741F04C9853D9797CF
SHA1:	FE187847ADBF96DB39301A1C1B04F30E3E3DB4E9
SHA-256:	EA37623DB683B059EFA3CB4954B86124F93301F3EC41F6CBDF0AED05298AEF88
SHA-512:	C8B0C4ADA17F15A753BF1CB71F3BDD3AF5A23FF1BBDED1427B41BFB9105AE34AE62227D30B899FC9C4897A1F8C4C59CFD531BB4A636837929279F5C9A734C394
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....K..`.....U.....B.....D .....GenuineIntelW.....T.....I..`.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... .....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8268
Entropy (8bit):	3.6953250354060008
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiMg6B6YAU6A2AgmfTZSBCprRx89bYQsf+Im:RrlsNir6B6Yj6A2AgmfTZSGeYjf4
MD5:	E3D77CF53ECF7ADB317D3A435DCD8159
SHA1:	D28D76FE62068ACB5D8F00D79923955617DB9998
SHA-256:	65DF5D85CE9B5BCABAD28554C8A00324EA2271DC2FD9464ADC2058E1D726619F
SHA-512:	5A297AC88ED72FFC3493E4072759293A4B52302719ECEE00A6B78070D63F7C4CC595C13ABE25E9F96149ACA7F3CC1593AF54248A772EED1DDC2C019AE2FF0693
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4DF0.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4629
Entropy (8bit):	4.472021705479319
Encrypted:	false
SSDEEP:	48:cvIwSD8zsxBJgtWI9G4WSC8BK8fm8M4JCdsfFD3+q8/o64SrSOd:uITfVdxSNNJr3KDWOd
MD5:	11E5F02DEF35759B3C71A7D954F0F740
SHA1:	BAE0F45B66F1045B6D690D071B391A1BC3D68F70
SHA-256:	D7AAABAB2E17E78EC0F35AC3A9E23CBBBA452F34E44C07E5A0F0F03B8CDAF03E
SHA-512:	9E84C713910BE1D55E4D061C54D97C8CDA5075C231D0126A02D356BE37CD59949DC10C55A9D8DE80761CCB8760E969CD182417B3B07D5165034963718434AA4

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4DF0.tmp.xml	
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="839973" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Jan 30 22:23:12 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	50486
Entropy (8bit):	2.1510325720772263
Encrypted:	false
SSDEEP:	192:4i5J9Tm4BswRJDrI/QtC0cyflT5wkMQGd2K/WjZvB4Zp6w+jtgief6nLd:PJ9TmHwRJHQ3gO27VvqrF+jtASLd
MD5:	8408AA93B0C2C7F26D17D6D77B2C9832
SHA1:	63DA04E109DD39C3848A024E5E6BA1A3531F4D4B
SHA-256:	C99BD6708DD3A2B4C06BB07717D57723437098322F361CF951A41258210E99E7
SHA-512:	980E2D62707C2278EAF476907E7F7DA4801CC6D6FAA1F37A2C1D8A0238B0A6A80875C516B34B6054326BDD7859988AAF1B24E4DA64BE25AAB598A29BEBA89C0 1
Malicious:	false
Preview:	MDMP..... .....P..`.....U.....B.....D .....GenuineIntelW.....T.....\...L..`.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8248
Entropy (8bit):	3.693363910446504
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNilM86F6YAg6ApgmfTuSBCpr989bDlsfMBm:RrlsNiF6F6YP6ApgmfTuSLD+fH
MD5:	A6CB8208BC27FA8FBA080B2E4D8BDD71
SHA1:	6215C7F1D310652F0A034ABAFF81E47DDC288508
SHA-256:	B762FAE10CCC9B0C448F8C9AED1AD334E847C464595377410972690F4AB6AEA1
SHA-512:	669B97305AC45D8D85B1A173C4ACE63AC58042570F0C7BCCC2850D6BA7D075D6989069896ACFA94071515F3F1B070AB4D20AE98263834F2387F2E79639615609
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.0.4.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F65.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4629
Entropy (8bit):	4.4740213509877185
Encrypted:	false
SSDEEP:	48:cvIwSD8zsxBJgtWI9G4WSC8Bq28fm8M4JCdsUFoi+q8/oqq4SrSBd:uITfVdxSNMJoaqDWBd
MD5:	33574F790F04EE4F15C8FD5D7F13B70F
SHA1:	D52A243595682BD5C96A40824A2D9B1475A8411D
SHA-256:	88413B191DD655B8B29D8FE0A469109C8867D9E8E97766F7B2D8F146067F7D95
SHA-512:	4E9040A48134C860CFE35DD67EE6FBFF8DF44B86ABC739B384CFD1F266A5D532B82B7E8F8B63CBF3502C0080B025F0E3FEECA9C01E139CA75F1542A504C2E3 5
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F65.tmp.xml	
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="839973" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.4522280470694
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	A8xYhQFvXo.dll
File size:	4890624
MD5:	83dd317c95f4acb8623d1f024945cfdb
SHA1:	04f9227cc3bfde5626be669be106a5d38f4416b1
SHA256:	5b2f060f1512100a0d500312fa579cdad9d3ea101778838173aa7215cd39700a
SHA512:	93cddc6bb6957e38d2485bea380d19b8291d3069d78e03cff58a792a5d6c5a56b983b34f166379a0ff9d1e009a461f71c21a59e98de8081503d9364ad91deb41
SSDEEP:	98304:jEn4O4Kkolx67k+Yj6i7SVSVSRDEdxA0L6EwSls/9kXUVje32C:jE4O4KW4rj6ESVSVSR/i6Ewb98d2C
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....JG ..&N..&N..&N.....&N...0..&N.).3./&N.). .@&N.).#.9'N..)...&N..)...&N..&O.4'N.).<.I&N.).4..&N.).2..&N.).6..&N.Rich.&N.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100288f0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x5F9F5377 [Mon Nov 2 00:31:51 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	7438c2384f3e113e7ab9f88b1b5e5108

Entrypoint Preview

Instruction
cmp dword ptr [esp+08h], 01h
jne 00007EFCF482E9C7h
call 00007EFCF483A812h
push dword ptr [esp+04h]
mov ecx, dword ptr [esp+10h]
mov edx, dword ptr [esp+0Ch]
call 00007EFCF482E8B2h
pop ecx
retn 000Ch
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 10171808h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
test eax, eax
pop edi
mov dword ptr [ebp-04h], eax
pop esi
je 00007EFCF482E9CEh
test byte ptr [eax], 00000008h
je 00007EFCF482E9C9h
mov dword ptr [ebp-0Ch], 01994000h
lea eax, dword ptr [ebp-0Ch]
push eax
push dword ptr [ebp-10h]
push dword ptr [ebp-1Ch]
push dword ptr [ebp-20h]
call dword ptr [10171320h]
leave
retn 0008h
push ebp
mov ebp, esp
push ecx
push ebx
mov eax, dword ptr [ebp+0Ch]
add eax, 0Ch
mov dword ptr [ebp-04h], eax
mov ebx, dword ptr fs:[00000000h]
mov eax, dword ptr [ebx]
mov dword ptr fs:[00000000h], eax
mov eax, dword ptr [ebp+08h]
mov ebx, dword ptr [ebp+0Ch]
mov ebp, dword ptr [ebp-04h]
mov esp, dword ptr [ebx-04h]
jmp eax
pop ebx
leave
retn 0008h
pop eax
pop ecx
xchg dword ptr [esp], eax
jmp eax
push ebp
mov ebp, esp
push ecx
push ecx

Instruction
push ebx
push esi
push edi
mov esi, dword ptr fs:[00000000h]
mov dword ptr [ebp-04h], esi
mov dword ptr [ebp-08h], 100289BBh
push 00000000h
push dword ptr [ebp+0Ch]
push dword ptr [ebp-08h]
push dword ptr [ebp+08h]
call 00007EFCF482E9E2h

Rich Headers

Programming Language:	• [RES] VS2005 build 50727 • [C] VS2005 build 50727 • [EXP] VS2005 build 50727 • [C++] VS2005 build 50727 • [ASM] VS2005 build 50727 • [LNK] VS2005 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x288570	0x6e	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x286c3c	0x118	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x409000	0x98db0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x4a2000	0xb370	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x27b658	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x171000	0x4dc	.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	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x16ff8b	0x170000	False	0.486878104832	data	6.46262078477	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x171000	0x1175de	0x118000	False	0.4536996024	data	6.46893668097	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x289000	0x17f0e4	0x179000	False	0.952282488188	data	7.96722658693	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x409000	0x98db0	0x99000	False	0.999259599673	data	7.99961057955	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x4a2000	0xea20	0xf000	False	0.511735026042	data	5.63038298318	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
CRX	0x409150	0x9369	7-zip archive data, version 0.3	English	United States
FF	0x4124bc	0x87050	7-zip archive data, version 0.3	English	United States
FRIENDS	0x49950c	0x884a	7-zip archive data, version 0.3	English	United States
RT_MANIFEST	0x4a1d58	0x56	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFilePointer, MapViewOfFile, UnmapViewOfFile, SetEndOfFile, HeapAlloc, QueryPerformanceCounter, HeapFree, WaitForSingleObject, InterlockedCompareExchange, UnlockFile, FlushViewOfFile, LockFile, WaitForSingleObjectEx, OutputDebugStringW, GetTickCount, UnlockFileEx, GetProcessHeap, GetSystemTimeAsFileTime, FormatMessageA, InitializeCriticalSection, LoadLibraryW, FormatMessageW, HeapDestroy, LeaveCriticalSection, GetFileAttributesA, HeapCreate, HeapValidate, GetFileAttributesW, FlushFileBuffers, GetTempPathW, HeapSize, LockFileEx, EnterCriticalSection, GetDiskFreeSpaceW, CreateFileMappingA, CreateFileMappingW, GetDiskFreeSpaceA, GetSystemInfo, GetFileAttributesExW, DeleteCriticalSection, GetCurrentThreadId, GetVersionExA, DeleteFileW, HeapCompact, GetTempPathA, AreFileApisANSI, WinExec, GetPrivateProfileStringA, CreateSemaphoreA, VirtualFree, VirtualAlloc, GetLocalTime, OpenFileMappingA, lstrcpynA, CopyFileA, SetFileAttributesA, FindResourceA, LoadResource, SizeofResource, MoveFileA, LockResource, GetWindowsDirectoryA, GetThreadContext, SetThreadContext, VirtualAllocEx, GetModuleHandleA, WriteProcessMemory, ResumeThread, GetThreadLocale, GetFileInformationByHandle, GetDriveTypeA, FileTimeToLocalFileTime, FileTimeToSystemTime, CreateMutexW, HeapReAlloc, GetFullPathNameA, GetFullPathNameW, GetModuleHandleW, DeviceIoControl, CreateFileW, GetVersionExW, GetVolumeInformationW, GetSystemDirectoryW, GetComputerNameW, OutputDebugStringA, DeleteFileA, GetSystemTime, LocalFree, CloseHandle, CreateMutexA, FindNextFileA, LocalAlloc, OpenMutexA, LoadLibraryA, FindClose, GetProcAddress, GetLastError, FindFirstFileA, MultiByteToWideChar, GetTimeZoneInformation, ReadFile, CreateProcessA, WideCharToMultiByte, WriteFile, CompareFileTime, GetCurrentProcess, SystemTimeToFileTime, FreeLibrary, lstrlenA, GetFileSize, CreateFileA, GetStringTypeExA, GetSystemDirectoryA, ExpandEnvironmentStringsA, WaitForMultipleObjects, PeekNamedPipe, SleepEx, SetCurrentDirectoryA, SetFileTime, SetFileAttributesW, CreateDirectoryW, GetCurrentDirectoryA, SetEnvironmentVariableA, GetCurrentProcessId, Sleep, CompareStringW, CompareStringA, WriteConsoleW, GetConsoleOutputCP, WriteConsoleA, SetStdHandle, GetLocaleInfoW, IsValidCodePage, IsValidLocale, EnumSystemLocalesA, GetLocaleInfoA, GetUserDefaultLCID, GetStringTypeW, GetStringTypeA, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetEnvironmentStrings, FreeEnvironmentStringsA, GetConsoleMode, GetConsoleCP, GetStartupInfoA, GetFileType, SetHandleCount, GetModuleFileNameA, GetStdHandle, ExitProcess, InterlockedIncrement, InterlockedDecrement, InterlockedExchange, TerminateProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, CreateDirectoryA, ExitThread, CreateThread, GetCommandLineA, RaiseException, RtlUnwind, GetCPInfo, LCMapStringA, LCMapStringW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetACP, GetOEMCP
USER32.dll	wsprintfA, LoadStringA, wsprintfW, GetSystemMetrics
ADVAPI32.dll	GetSidIdentifierAuthority, CryptDestroyKey, CryptEncrypt, CryptReleaseContext, CryptImportKey, CryptAcquireContextA, GetSecurityDescriptorSacl, SetSecurityInfo, ControlService, OpenSCManagerA, StartServiceA, CreateServiceA, DeleteService, CloseServiceHandle, OpenServiceA, LookupAccountNameW, GetSidSubAuthorityCount, GetSidSubAuthority, CryptCreateHash, RegCloseKey, RegEnumKeyExW, RegOpenKeyExW, RegOpenKeyExA, RegCreateKeyExA, SetSecurityDescriptorDacl, InitializeSecurityDescriptor, RegQueryValueExW, LookupAccountSidA, RegQueryValueExA, RegSetValueExA, GetTokenInformation, OpenProcessToken, CryptDestroyHash, CryptGetHashParam, CryptHashData
SHELL32.dll	SHGetPathFromIDListA, SHGetMalloc, SHGetSpecialFolderLocation, SHFileOperationA, SHGetSpecialFolderPathA
ole32.dll	CoInitialize, CoUninitialize, CoCreateInstance
SHLWAPI.dll	PathFindFileNameA, PathRemoveFileSpecA, PathFileExistsA, SHGetValueA
WS2_32.dll	getpeername, closesocket, socket, connect, sendto, recvfrom, accept, listen, inet_addr, gethostbyname, inet_ntoa, getservbyname, gethostbyaddr, getservbyport, ioctlsocket, gethostname, getsockopt, htons, bind, ntohs, setsockopt, WSAIoctl, select, __WSAFDIsSet, WSASetLastError, send, recv, WSAGetLastError, WSAStartup, WSACleanup, htonl, getsockname, ntohl
CRYPT32.dll	CryptUnprotectData
VERSION.dll	GetFileVersionInfoA, GetFileVersionInfoSizeA, VerQueryValueA
WINHTTP.dll	WinHttpAddRequestHeaders, WinHttpQueryOption, WinHttpReceiveResponse, WinHttpSetTimeouts, WinHttpSetOption, WinHttpSendRequest, WinHttpConnect, WinHttpCloseHandle, WinHttpQueryHeaders, WinHttpQueryDataAvailable, WinHttpOpen, WinHttpOpenRequest, WinHttpReadData, WinHttpSetCredentials
WININET.dll	InternetGetCookieExA, InternetGetCookieA
SETUPAPI.dll	SetupDiGetDeviceRegistryPropertyA, SetupDiEnumDeviceInfo, SetupDiDestroyDeviceInfoList, SetupDiGetClassDevsA
WLDAP32.dll	

Exports

Name	Ordinal	Address
Hello001	1	0x10148400
Hello002	2	0x10148370
Hello003	3	0x10148300

Possible Origin

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

Network Behavior

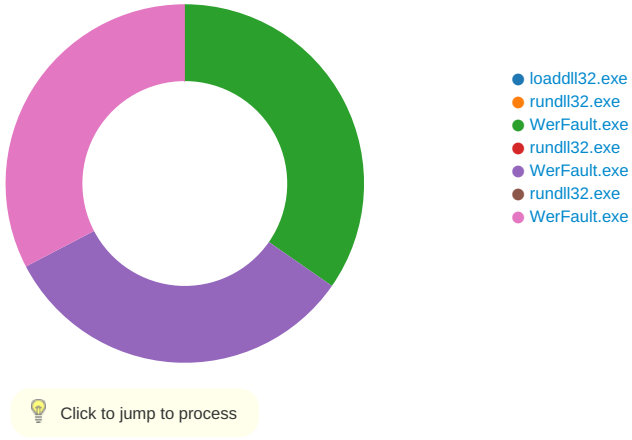
UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2021 14:22:57.140047073 CET	55984	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:22:57.199223042 CET	53	55984	8.8.8.8	192.168.2.3
Jan 30, 2021 14:22:58.107640028 CET	64185	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:22:58.155550957 CET	53	64185	8.8.8.8	192.168.2.3
Jan 30, 2021 14:22:59.079483032 CET	65110	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:22:59.130264997 CET	53	65110	8.8.8.8	192.168.2.3
Jan 30, 2021 14:23:00.114022017 CET	58361	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:23:00.171459913 CET	53	58361	8.8.8.8	192.168.2.3
Jan 30, 2021 14:23:01.126566887 CET	63492	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:23:01.185852051 CET	53	63492	8.8.8.8	192.168.2.3
Jan 30, 2021 14:23:02.291366100 CET	60831	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:23:02.339575052 CET	53	60831	8.8.8.8	192.168.2.3
Jan 30, 2021 14:23:03.112068892 CET	60100	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:23:03.164654016 CET	53	60100	8.8.8.8	192.168.2.3
Jan 30, 2021 14:23:04.301146030 CET	53195	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:23:04.349097967 CET	53	53195	8.8.8.8	192.168.2.3
Jan 30, 2021 14:23:05.443454981 CET	50141	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:23:05.495985985 CET	53	50141	8.8.8.8	192.168.2.3
Jan 30, 2021 14:23:06.295280933 CET	53023	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:23:06.353816032 CET	53	53023	8.8.8.8	192.168.2.3
Jan 30, 2021 14:23:06.400911093 CET	49563	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:23:06.448723078 CET	53	49563	8.8.8.8	192.168.2.3
Jan 30, 2021 14:23:09.283931971 CET	51352	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:23:09.332432985 CET	53	51352	8.8.8.8	192.168.2.3
Jan 30, 2021 14:23:10.654191971 CET	59349	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:23:10.708065033 CET	53	59349	8.8.8.8	192.168.2.3
Jan 30, 2021 14:23:11.519303083 CET	57084	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:23:11.568506002 CET	53	57084	8.8.8.8	192.168.2.3
Jan 30, 2021 14:23:12.727240086 CET	58823	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:23:12.777928114 CET	53	58823	8.8.8.8	192.168.2.3
Jan 30, 2021 14:23:13.687099934 CET	57568	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:23:13.734935999 CET	53	57568	8.8.8.8	192.168.2.3
Jan 30, 2021 14:23:13.957366943 CET	50540	53	192.168.2.3	8.8.8.8
Jan 30, 2021 14:23:14.016382933 CET	53	50540	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6628 Parent PID: 5680

General

Start time:	14:23:01
Start date:	30/01/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\A8xYhQFvXo.dll'
Imagebase:	0x1240000
File size:	120832 bytes
MD5 hash:	2D39D4DFDE8F7151723794029AB8A034
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6652 Parent PID: 6628

General

Start time:	14:23:01
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\A8xYhQFvXo.dll,Hello001
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000001.00000002.230780419.000000001028B000.00000008.00020000.sdmp, Author: Florian Roth
Reputation:	high

Analysis Process: WerFault.exe PID: 6708 Parent PID: 6652

General

Start time:	14:23:03
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6652 -s 712
Imagebase:	0x12b0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true

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

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E031717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER413E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER413E.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_9155b230567b23dc90309f27732428df1d2d4b15_82810a17_1a0b4812	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_9155b230567b23dc90309f27732428df1d2d4b15_82810a17_1a0b4812\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E02497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER413E.tmp	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	success or wait	1	6E024BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	success or wait	1	6E024BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER413E.tmp.xml	success or wait	1	6E024BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A58.tmp.csv	success or wait	1	6E024BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A79.tmp.txt	success or wait	1	6E024BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 48 dc 15 60 a4 05 12 00 00 00 00 00	MDMP..... .....H..`.....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 44 20 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 fc 19 00 00 45 dc 15 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B......D .... ..GenuineIntelW...........T... ....E..`.................. ....0..1.............. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 84 14 10 c8 34 bc 00 00 f8 83 00 c2 00 20 00 c2 00 20 00 64 f8 83 00 8c 32 02 10 23 00 00 00 02 02 01 00 74 f6 83 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+............4........ ... . d....2..#.......t...+.........	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	168	00 1a 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 8c 32 02 10 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c2 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 20 26 00 00	........................2.... .... &..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	20	14 00 00 00 24 f7 ad 00 00 00 00 00 dc 08 00 00 60 35 00 00	....$...........`5..	success or wait	20	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	2268	bc b1 e5 77 d6 c9 e3 77 68 02 00 00 aa aa aa aa 10 00 00 00 b8 f7 ad 00 84 f8 ad 00 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 c0 6f 00 00 c0 6f 00 00 00 00 00 68 02 00 00 aa aa aa aa 68 02 00 00 aa aa aa aa 00 c0 6f 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 0e bd 00 00 00 00 00 00 00 00 00 50 07 bc 00 00 30 6f 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 74 fd ba 00 b8 f6 a4 00 e8 05 bc 00 c0 f6 a4 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...wh.................... ..@..w@..w......o...o.....h... ....h.........o.............. ....P....0o................ ....t.....	success or wait	19	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	4096	54 fe ba 00 00 00 bb 00 00 40 ba 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 f0 6f 00 00 00 00 00 fc 19 00 00 5c 1a 00 00 00 00 00 00 c8 10 bd 00 00 30 6f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 d6 77 09 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	T........@................o... ......\............0o......... ....p.w..............	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 f8 83 00 aa aa aa aa 00 00 00 00 08 e8 83 00 bc 9a e5 77 23 00 00 00 06 02 00 00 78 e6 83 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+........................... ....w#.......x...+.........	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	48	5c 1a 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 f0 6f 00 00 00 00 00 a8 fc ba 00 00 00 00 00 58 03 00 00 3c 3e 00 00 cc 02 00 00 50 31 00 00	\....... ....o.............X... <>......P1..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	4	34 00 00 00	4...	success or wait	52	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	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	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	52	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	752	00 00 48 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 06 26 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 b0 7b 02 00 00 00 00 00 40 ae 02 00 00 00 00 e3 28 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 75 4f 03 00 00 00 00 00 75 4f 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 81 7e 1b 00 00 00 00 00 bf 80 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 cd dc 04 00 00 00 00	..Ht.....0...U..s@...&..... .....B.....B?..... .....#..... ..@A.....Zb..... ....{.....@..... (.....uO.....uO .....~..... @.....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	10184	0a 00 00 00 45 00 76 00 65 00 6e 00 74 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 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	....E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e. t.i.o.n.P.a.c.k.e.t.....I.o. C.o.m.p.l.e.t.i.o.n.....T.p. W.o.r.k.e.r.F.a.c.t.o.r.y..... ..I.R.T.i.m.e.r...(...W.a.i.t. C.o.m.p.l.e.t.i.o.n.P.a.c.k.e. t.....I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3DB2.tmp.dmp	unknown	108	03 00 00 00 c4 00 00 00 fc 06 00 00 04 00 00 00 f4 15 00 00 cc 07 00 00 05 00 00 00 44 01 00 00 1c 34 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 58 1c 00 00 5c b8 00 00 15 00 00 00 ec 01 00 00 c0 1d 00 00 16 00 00 00 98 00 00 00 ac 1f 00 00	....4.....T.....8..... ....T.....X...\.....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.?.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.".?.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.W.E.R.R.e.p.o.r.t.M.e.t.a. d.a.t.a.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B. u.i.l.d.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 36 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.6.5.2.<./.P.i.d.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.I.m.a.g.e.N.a.m.e.>.r.u.n.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 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	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 30 00 34 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.0.4.8.<./.U.p.t.i.m.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	88	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 31 00 33 00 35 00 37 00 31 00 36 00 38 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	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.3.5.7.1.6.8.6.4.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	72	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 31 00 33 00 35 00 37 00 31 00 36 00 38 00 36 00 34 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	<.V.i.r.t.u.a.l.S.i.z.e.>.1.3.5.7.1.6.8.6.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 37 00 30 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.0.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 39 00 30 00 39 00 37 00 32 00 31 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	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.0.9.7.2.1.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 39 00 30 00 39 00 37 00 32 00 31 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.0.9.7.2.1.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 32 00 30 00 30 00 30 00 35 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 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	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.0.0.5.8.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 32 00 30 00 30 00 33 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	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.0.0.3.1.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 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 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	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.7.5.1.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 35 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.7.5.1.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 37 00 32 00 33 00 37 00 36 00 33 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	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.2.3.7.6.3.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 37 00 32 00 33 00 37 00 36 00 33 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	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.2.3.7.6.3.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 37 00 32 00 33 00 37 00 36 00 33 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	<.P.r.i.v.a.t.e.U.s.a.g.e.>.7.2.3.7.6.3.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 36 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.6.2.8.<./.P.i.d.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 34 00 39 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.4.9.1.<./.U.p.t.i.m.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 39 00 34 00 33 00 34 00 34 00 39 00 36 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	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.9.9.4.3.4.4.9.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 36 00 37 00 31 00 34 00 37 00 35 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.9.6.7.1.4.7.5.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 39 00 34 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.9.4.3.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 33 00 39 00 37 00 33 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	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.3.9.7.3.7.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 33 00 33 00 35 00 39 00 33 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.3.3.5.9.3.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 39 00 31 00 33 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.9.1.3.6.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 38 00 33 00 34 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	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.3.4.9.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 30 00 38 00 30 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.8.0.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 30 00 35 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.5.2.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 33 00 32 00 31 00 31 00 32 00 36 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	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.2.1.1.2.6.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 33 00 32 00 31 00 35 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.2.1.5.3.6.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 33 00 32 00 31 00 31 00 32 00 36 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	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.2.1.1.2.6.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	74	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 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	<.P.a.r.a.m.e.t.e.r.0.>.r.u.n.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 75 00 75 00 6c 00 67 00 6a 00 6a 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	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.u.u.l.g.j.j.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 75 00 75 00 6c 00 67 00 6a 00 6a 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.u.u.l.g.j.j.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 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	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 35 00 34 00 38 00 36 00 39 00 36 00 36 00 32 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	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.4.8.6.9.6.6.2.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 31 00 2d 00 33 00 30 00 54 00 32 00 32 00 3a 00 32 00 33 00 3a 00 30 00 35 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.1.-.3.0.T.2.2.:.2.3.:.0.5.Z.".>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	258	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 33 00 34 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 36 00 35 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 33 00 37 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 33 00 37 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.4.2.". .P.I.D.=.".6.6.5.2.". .U.p.t.i.m.e.M.S.=.".4.3.7.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".4.3.7.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 34 00 39 00 30 00 30 00 63 00 37 00 37 00 2d 00 39 00 62 00 33 00 32 00 2d 00 34 00 66 00 63 00 64 00 2d 00 61 00 32 00 61 00 33 00 2d 00 64 00 30 00 36 00 37 00 34 00 33 00 62 00 61 00 32 00 65 00 33 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.f.4.9.0.0.c.7.7.-.9.b.3.2.-.4.f.c.d.-.a.2.a.3.-.d.0.6.7.4.3.b.a.2.e.3.b.<./.G.u.i.d.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 31 00 2d 00 33 00 30 00 54 00 32 00 32 00 3a 00 32 00 33 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	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.1.-.3.0.T.2.2.:.2.3.:.0.5.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4043.tmp.WERInternalMetadata.xml	unknown	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	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER413E.tmp.xml	unknown	4629	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_9155b230567b23dc90309f27732428df1d2d4b15_82810a17_1a0b4812\Report.wer	unknown	2	ff fe	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_9155b230567b23dc90309f27732428df1d2d4b15_82810a17_1a0b4812\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	183	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_9155b230567b23dc90309f27732428df1d2d4b15_82810a17_1a0b4812\Report.wer	unknown	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 36 00 34 00 36 00 37 00 33 00 34 00 30 00 38 00 33 00	M.e.t.a.d.a.t.a.H.a.s.h.=.6.4.6.7.3.4.0.8.3.	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6E0436BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6E041FB2	RegCreateKeyExW
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0243D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6E0436BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6E0436BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 8C 32 02 10 02 00 00 00 00 00 00 00 C2 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E041FE8	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6896 Parent PID: 6628

General

Start time:	14:23:05
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\A8xYhQFvXo.dll,Hello002
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000004.00000002.236067014.000000001028B000.00000008.00020000.sdmp, Author: Florian Roth
Reputation:	high

Analysis Process: WerFault.exe PID: 6972 Parent PID: 6896

General

Start time:	14:23:06
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6896 -s 712
Imagebase:	0x12b0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E031717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4DF0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4DF0.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5a155b1e9b8901355626d9881b9ed599cf1223_82810a17_1b0352d0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5a155b1e9b8901355626d9881b9ed599cf1223_82810a17_1b0352d0\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E02497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp	success or wait	1	6E02497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4DF0.tmp	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	success or wait	1	6E024BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	success or wait	1	6E024BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4DF0.tmp.xml	success or wait	1	6E024BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA6ED.tmp.csv	success or wait	1	6E024BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA70D.tmp.txt	success or wait	1	6E024BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 4b dc 15 60 a4 05 12 00 00 00 00 00	MDMP..... .....K..`.....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 44 20 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 f0 1a 00 00 49 dc 15 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	.....U.....B.....D .... ..GenuineIntelW.....T... .....I..`..... .....0..1..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 70 83 14 10 c8 34 16 03 00 f5 c7 00 24 01 06 00 24 01 06 00 f4 f5 c7 00 b0 32 02 10 23 00 00 00 46 02 01 00 04 f4 c7 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.......p....4......$...$... .....2..#...F.......+.........	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	168	f4 1a 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 b0 32 02 10 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 01 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 20 26 00 00	.........................2.... ....$........... .... &..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	20	11 00 00 00 20 f8 e5 00 00 00 00 00 e0 07 00 00 30 35 00 00	....05..	success or wait	17	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	2016	bc b1 e5 77 d6 c9 e3 77 5c 02 00 00 aa aa aa aa 10 00 00 00 b4 f8 e5 00 80 f9 e5 00 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 10 a3 00 00 10 a3 00 00 00 00 00 5c 02 00 00 aa aa aa aa 5c 02 00 00 aa aa aa aa 00 10 a3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 c7 15 03 00 00 00 00 00 00 00 00 50 07 16 03 00 b0 a2 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa bc f6 f1 00 54 b2 a2 00 c4 f6 f1 00 e8 05 16 03 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...w\..................... ..@..w@..w................\... ....\......................... ....P....................... ....T.	success or wait	16	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	7164	bc 9a e5 77 a3 1a 21 75 aa aa aa aa 38 e6 c7 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 c4 02 00 00 c0 02 00 00 00 00 00 00 24 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 b0 a2 00 00 00 00 00 00 00 00 00 00 00 00 00 38 e6 c7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w..!u....8................. ....$........... ....8...............	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 f5 c7 00 aa aa aa aa 00 00 00 00 98 e5 c7 00 bc 9a e5 77 23 00 00 00 02 02 00 00 08 e4 c7 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+.......................... ....w#...........+.........	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	48	10 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 70 a3 00 00 00 00 00 48 f9 89 04 00 00 00 00 b8 06 00 00 20 47 00 00 cc 02 00 00 50 31 00 00	....p......H.......... G......P1..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	4	34 00 00 00	4...	success or wait	52	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	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	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	52	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	752	00 00 48 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 06 26 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 e0 84 02 00 00 00 00 00 40 ae 02 00 00 00 00 78 54 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 9b 65 03 00 00 00 00 00 00 9c 65 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8f 2f 18 00 00 00 00 00 b1 cf 07 00 00 00 00 00 40 ff 1f 00 00 00 00 00 40 e2 07 00 00 00 00	..Ht.....0...U..s@...&..... .....B.....B?..... .....#..... ..@A.....Zb..... ....@..... xT.....e.....e ...../..... @.....@.....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	10184	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 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 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	....E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e. t.i.o.n.P.a.c.k.e.t.....I.o. C.o.m.p.l.e.t.i.o.n.....T.p. W.o.r.k.e.r.F.a.c.t.o.r.y..... ..I.R.T.i.m.e.r...(...W.a.i.t. C.o.m.p.l.e.t.i.o.n.P.a.c.k.e. t.....I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER493B.tmp.dmp	unknown	108	03 00 00 00 c4 00 00 00 fc 06 00 00 04 00 00 00 f4 15 00 00 cc 07 00 00 05 00 00 00 14 01 00 00 1c 34 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 58 1c 00 00 f0 bc 00 00 15 00 00 00 ec 01 00 00 c0 1d 00 00 16 00 00 00 98 00 00 00 ac 1f 00 00	....4.....T.....8..... ....T.....X.....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.?.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.".?.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.W.E.R.R.e.p.o.r.t.M.e.t.a. d.a.t.a.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B. u.i.l.d.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.8.9.6.<./.P.i.d.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.I.m.a.g.e.N.a.m.e.>.r.u.n.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 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	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 38 00 34 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.8.4.2.<./.U.p.t.i.m.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	88	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 31 00 33 00 35 00 37 00 32 00 35 00 30 00 35 00 36 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	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.3.5.7.2.5.0.5.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	72	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 31 00 33 00 35 00 37 00 31 00 36 00 38 00 36 00 34 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	<.V.i.r.t.u.a.l.S.i.z.e.>.1.3.5.7.1.6.8.6.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 37 00 31 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	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.1.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 39 00 31 00 30 00 35 00 34 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.1.0.5.4.0.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 39 00 31 00 30 00 35 00 34 00 30 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	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.1.0.5.4.0.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 32 00 30 00 30 00 30 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	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.0.0.5.1.2.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 32 00 30 00 30 00 33 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	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.0.0.3.1.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.8.0.7.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 38 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.7.8.0.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 37 00 32 00 34 00 31 00 37 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.2.4.1.7.2.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 37 00 32 00 34 00 39 00 39 00 32 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	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.2.4.9.9.2.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 37 00 32 00 34 00 31 00 37 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.7.2.4.1.7.2.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 36 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.6.2.8.<./.P.i.d.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 36 00 30 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.6.6.0.0.<./.U.p.t.i.m.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	88	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 31 00 30 00 30 00 37 00 34 00 35 00 32 00 31 00 36 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	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.0.0.7.4.5.2.1.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 36 00 37 00 31 00 34 00 37 00 35 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.9.6.7.1.4.7.5.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 39 00 37 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	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.9.7.5.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 34 00 34 00 32 00 34 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.4.4.2.4.3.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 33 00 33 00 35 00 39 00 33 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.3.3.5.9.3.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 39 00 31 00 33 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.9.1.3.6.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 38 00 33 00 34 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	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.3.4.9.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 31 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.1.0.7.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 30 00 35 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.5.2.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 33 00 32 00 31 00 31 00 32 00 36 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	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.2.1.1.2.6.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 33 00 32 00 31 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	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.2.1.9.4.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 33 00 32 00 31 00 31 00 32 00 36 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	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.2.1.1.2.6.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	74	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 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	<.P.a.r.a.m.e.t.e.r.0.>.r.u.n.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 75 00 75 00 6c 00 67 00 6a 00 6a 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	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.u.u.l.g.j.j.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 75 00 75 00 6c 00 67 00 6a 00 6a 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.u.u.l.g.j.j.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 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	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 35 00 34 00 38 00 36 00 39 00 36 00 36 00 32 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	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.4.8.6.9.6.6.2.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 31 00 2d 00 33 00 30 00 54 00 32 00 32 00 3a 00 32 00 33 00 3a 00 30 00 38 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.1.-.3.0.T.2.2.:.2.3.:.0.8.Z.".>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	258	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 33 00 34 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 38 00 39 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 34 00 30 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 30 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.4.6.". .P.I.D.=.".6.8.9.6.". .U.p.t.i.m.e.M.S.=.".4.0.6.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".4.0.6.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 65 00 36 00 61 00 39 00 38 00 39 00 36 00 2d 00 31 00 35 00 36 00 36 00 2d 00 34 00 61 00 63 00 35 00 2d 00 39 00 39 00 38 00 32 00 2d 00 62 00 33 00 64 00 39 00 37 00 65 00 64 00 61 00 65 00 65 00 31 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.3.e.6.a.9.8.9.6.-.1.5.6.6.-.4.a.c.5.-.9.9.8.2.-.b.3.d.9.7.e.d.a.e.e.1.c.<./.G.u.i.d.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 31 00 2d 00 33 00 30 00 54 00 32 00 32 00 3a 00 32 00 33 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	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.1.-.3.0.T.2.2.:.2.3.:.0.8.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4C88.tmp.WERInternalMetadata.xml	unknown	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	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4DF0.tmp.xml	unknown	4629	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5a155b1e9b8901355626d9881b9ed599cf1223_82810a17_1b0352d0\Report.wer	unknown	2	ff fe	..	success or wait	1	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5a155b1e9b8901355626d9881b9ed599cf1223_82810a17_1b0352d0\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	183	6E02497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5a155b1e9b8901355626d9881b9ed599cf1223_82810a17_1b0352d0\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 35 00 32 00 37 00 35 00 31 00 33 00 38 00 32 00 39 00	M.e.t.a.d.a.t.a.H.a.s.h.=.5.2.7.5.1.3.8.2.9.	success or wait	1	6E02497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0436BF	unknown
\REGISTRY\A\{434a4e0a-487b-9225-eeaa-ed376b398141}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6E0243D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 8C 32 02 10 02 00 00 00 00 00 00 00 C2 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 B0 32 02 10 02 00 00 00 00 00 00 00 24 01 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E041FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: 7004 Parent PID: 6628

General

Start time:	14:23:08
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\A8xYhQFvXo.dll,Hello003
Imagebase:	0xf50000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000007.00000002.245505715.000000001028B000.00000008.00020000.sdmp, Author: Florian Roth
Reputation:	high

Analysis Process: WerFault.exe PID: 7092 Parent PID: 7004

General

Start time:	14:23:11
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7004 -s 712
Imagebase:	0x12b0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	701C1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F65.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F65.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_9155b230567b23dc90309f27732428df1d2d4b15_82810a17_1b8b63b8	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_9155b230567b23dc90309f27732428df1d2d4b15_82810a17_1b8b63b8\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	701B497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F65.tmp	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	success or wait	1	701B4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	success or wait	1	701B4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F65.tmp.xml	success or wait	1	701B4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB883.tmp.csv	success or wait	1	701B4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB8A3.tmp.txt	success or wait	1	701B4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 50 dc 15 60 a4 05 12 00 00 00 00 00	MDMP..... .....P..`.....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 44 20 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 5c 1b 00 00 4c dc 15 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B......D .... ..GenuineIntelW...........T... ....\...L..`.................. ....0..1............... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 83 14 10 c8 34 59 03 00 08 05 05 c2 00 23 00 c2 00 23 00 a8 fc 29 03 8c 32 02 10 23 00 00 00 02 02 01 00 b8 fa 29 03 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+............4Y.......#...#. ..)..2..#.........).+.........	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	168	60 1b 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 8c 32 02 10 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c2 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 20 26 00 00	`........................2.... ....#......... .... &..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	20	12 00 00 00 c0 ea 25 03 00 00 00 00 04 00 00 00 40 35 00 00	......%.........@5..	success or wait	18	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	4	dc 95 e5 77	...w	success or wait	17	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	4	94 fd e9 04	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 50 ec 29 03 bc 9a e5 77 23 00 00 00 16 02 00 00 c0 ea 29 03 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+.......................... P.)....w#.........).+.........	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	48	78 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 40 1b 03 00 00 00 00 c8 fc e9 04 00 00 00 00 38 03 00 00 cc 9a 00 00 cc 02 00 00 50 31 00 00	x....... ....@........... ..8...........P1..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	4	34 00 00 00	4...	success or wait	52	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	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	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	52	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	752	00 00 48 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 06 26 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 a0 71 02 00 00 00 00 00 40 ae 02 00 00 00 00 52 55 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 92 6d 03 00 00 00 00 00 59 6f 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f a1 0b 00 00 00 00 00 21 5e 14 00 00 00 00 00 40 ff 1f 00 00 00 00 00 81 62 14 00 00 00 00	..Ht.....0...U..s@...&..... .....B.....B?..... .....#..... ..@A.....Zb..... ....q.....@..... RU.....m.....Yo .....!^..... @.....b.....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	10086	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 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 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	....E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e. t.i.o.n.P.a.c.k.e.t.....I.o. C.o.m.p.l.e.t.i.o.n.....T.p. W.o.r.k.e.r.F.a.c.t.o.r.y..... ..I.R.T.i.m.e.r...(...W.a.i.t. C.o.m.p.l.e.t.i.o.n.P.a.c.k.e. t.....I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CB4.tmp.dmp	unknown	108	03 00 00 00 c4 00 00 00 fc 06 00 00 04 00 00 00 f4 15 00 00 cc 07 00 00 05 00 00 00 24 01 00 00 1c 34 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 30 1c 00 00 4e a9 00 00 15 00 00 00 ec 01 00 00 c0 1d 00 00 16 00 00 00 98 00 00 00 ac 1f 00 00	....4.....T.....8..... ....T.....0...N.....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.?.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.".?.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.W.E.R.R.e.p.o.r.t.M.e.t.a. d.a.t.a.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B. u.i.l.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.0.0.4.<./.P.i.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.I.m.a.g.e.N.a.m.e.>.r.u.n.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 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	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 32 00 37 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.2.7.9.<./.U.p.t.i.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	88	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 31 00 33 00 35 00 37 00 32 00 35 00 30 00 35 00 36 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	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.3.5.7.2.5.0.5.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	72	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 31 00 33 00 35 00 37 00 31 00 36 00 38 00 36 00 34 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	<.V.i.r.t.u.a.l.S.i.z.e.>.1.3.5.7.1.6.8.6.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 37 00 30 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.0.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 39 00 30 00 39 00 33 00 31 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.0.9.3.1.2.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 39 00 30 00 39 00 33 00 31 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.0.9.3.1.2.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 32 00 30 00 30 00 30 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	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.0.0.5.1.2.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 32 00 30 00 30 00 33 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	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.0.0.3.1.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.7.8.8.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 36 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	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.7.6.0.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 37 00 32 00 32 00 39 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.2.2.9.4.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 37 00 32 00 33 00 37 00 36 00 33 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	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.2.3.7.6.3.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 37 00 32 00 32 00 39 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.7.2.2.9.4.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 36 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.6.2.8.<./.P.i.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.I.m.a.g.e.N.a.m.e.>.(.u.n.a.b.l.e. .t.o. .r.e.t.r.i.e.v.e.).<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 32 00 32 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.1.1.2.2.5.<./.U.p.t.i.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	88	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 31 00 30 00 30 00 37 00 34 00 35 00 32 00 31 00 36 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	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.0.0.7.4.5.2.1.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.V.i.r.t.u.a.l.S.i.z.e.>.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 34 00 39 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.4.9.3.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 36 00 38 00 30 00 30 00 30 00 30 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	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.6.8.0.0.0.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 32 00 30 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	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.2.0.4.8.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 39 00 31 00 33 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.9.1.3.6.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 31 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.1.0.7.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	104	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 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.0.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.1.4.4.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 33 00 32 00 31 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	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.2.1.9.4.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.6.1.4.4.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	74	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 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	<.P.a.r.a.m.e.t.e.r.0.>.r.u.n.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 75 00 75 00 6c 00 67 00 6a 00 6a 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	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.u.u.l.g.j.j.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 75 00 75 00 6c 00 67 00 6a 00 6a 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.u.u.l.g.j.j.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 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	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 35 00 34 00 38 00 36 00 39 00 36 00 36 00 32 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	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.4.8.6.9.6.6.2.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 31 00 2d 00 33 00 30 00 54 00 32 00 32 00 3a 00 32 00 33 00 3a 00 31 00 32 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.1.-.3.0.T.2.2.:.2.3.:.1.2.Z.".>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 35 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 30 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 32 00 35 00 37 00 37 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 35 00 37 00 37 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.5.0.". .P.I.D.=.".7.0.0.4.". .U.p.t.i.m.e.M.S.=.".2.5.7.7.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".2.5.7.7.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=."	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 61 00 38 00 36 00 61 00 61 00 39 00 34 00 2d 00 36 00 32 00 64 00 37 00 2d 00 34 00 36 00 66 00 37 00 2d 00 61 00 37 00 33 00 31 00 2d 00 62 00 32 00 63 00 64 00 38 00 65 00 63 00 32 00 35 00 39 00 61 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.f.a.8.6.a.a.9.4.-.6.2.d.7.-.4.6.f.7.-.a.7.3.1.-.b.2.c.d.8.e.c.2.5.9.a.7.<./.G.u.i.d.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 31 00 2d 00 33 00 30 00 54 00 32 00 32 00 3a 00 32 00 33 00 3a 00 31 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	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.1.-.3.0.T.2.2.:.2.3.:.1.2.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5EA9.tmp.WERInternalMetadata.xml	unknown	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	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5F65.tmp.xml	unknown	4629	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_9155b230567b23dc90309f27732428df1d2d4b15_82810a17_1b8b63b8\Report.wer	unknown	2	ff fe	..	success or wait	1	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_9155b230567b23dc90309f27732428df1d2d4b15_82810a17_1b8b63b8\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	183	701B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_9155b230567b23dc90309f27732428df1d2d4b15_82810a17_1b8b63b8\Report.wer	unknown	42	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 31 00 37 00 34 00 32 00 34 00 31 00 35 00	M.e.t.a.d.a.t.a.H.a.s.h.=.2.1.7.4.2.4.1.5.	success or wait	1	701B497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0cec11a6-8435-aae0-63e1-089643899737}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701D36BF	unknown
\REGISTRY\A\{0cec11a6-8435-aae0-63e1-089643899737}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701D36BF	unknown
\REGISTRY\A\{0cec11a6-8435-aae0-63e1-089643899737}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701B43D1	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 B0 32 02 10 02 00 00 00 00 00 00 00 24 01 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 8C 32 02 10 02 00 00 00 00 00 00 00 C2 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	701D1FE8	RegSetValueExW

Disassembly

Code Analysis