ID: 404283
Sample Name:
fc0bc077_by_Libranalysis.dll
Cookbook: default.jbs
Time: 21:42:23
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

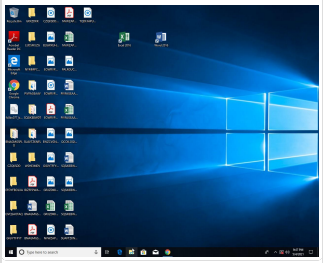
Analysis Report fc0bc077_by_Libranalysis.dll

Overview

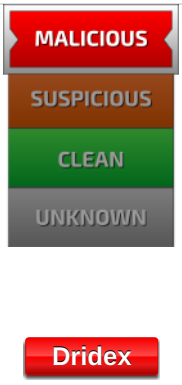
General Information

Sample Name:	fc0bc077_by_Libranalysis.dll
Analysis ID:	404283
MD5:	fc0bc07721ce94b..
SHA1:	2d98f05fb78cd75..
SHA256:	e707edac036a1a..
Tags:	Dridex
Infos:	

Most interesting Screenshot:



Detection

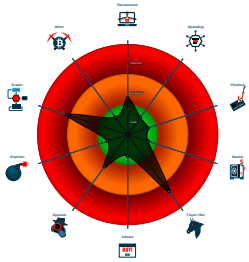


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Dridex unpacked file
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Tries to detect sandboxes / dynamic…
- Antivirus or Machine Learning detec…
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…
- Detected potential crypto function
- IP address seen in connection with o…
- Internet Provider seen in connection…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5980 cmdline: loaddll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5984 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4088 cmdline: rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 1848 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4088 -s 760 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 4860 cmdline: rundll32.exe C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll,LoxmtYt MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5852 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4860 -s 788 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5168 cmdline: rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',DllCanUnloadNow MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 4240 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5168 -s 752 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 4788 cmdline: rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',DllGetClassObject MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 3492 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4788 -s 760 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5188 cmdline: rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',WdiAddFileToInstance MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 1760 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5188 -s 756 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5204 cmdline: rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',WdiAddParameter MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5172 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5204 -s 756 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5220 cmdline: rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',WdiCancel MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 40112,
  "C2 list": [
    "193.200.130.181:443",
    "95.138.161.226:2303",
    "167.114.113.13:4125"
  ],
  "RC4 keys": [
    "MqW38NQIO70GhjGOOvjtl5AwyenW6A8fcZ",
    "xeMr6QHn7uRk1D2ChU8OuyaRFUZJZZHUIgxCzaPXtOkjmhTMtNxfWU8nlnD7q009ahEI51R1"
  ]
}
```

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_10f0240f\Report.wer	SUSP_WER_Critical_Heap Corruption	Detects a crashed application that crashed due to a heap corruption error (could be a sign of exploitation)	Florian Roth	• 0x11c:$a1: ReportIdentifier= • 0x19e:$a1: ReportIdentifier= • 0x77c:$a2: .Name=Fault Module Name • 0x92a:$s1: c0000374
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_0766ec0c\Report.wer	SUSP_WER_Critical_Heap Corruption	Detects a crashed application that crashed due to a heap corruption error (could be a sign of exploitation)	Florian Roth	• 0x11c:$a1: ReportIdentifier= • 0x19e:$a1: ReportIdentifier= • 0x77c:$a2: .Name=Fault Module Name • 0x92a:$s1: c0000374

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.326004095.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000014.00000002.480983725.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000010.00000002.489951685.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000011.00000002.489294314.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000013.00000002.488379155.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 1 entries				

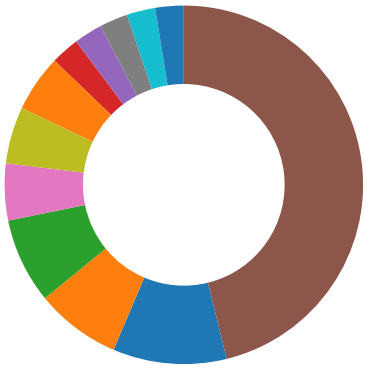
Unpacked PEs

Source	Rule	Description	Author	Strings
19.2.rundll32.exe.10000000.3.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
4.2.rundll32.exe.10000000.3.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
20.2.rundll32.exe.10000000.3.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
16.2.rundll32.exe.10000000.3.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
18.2.rundll32.exe.10000000.3.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Dridex unpacked file

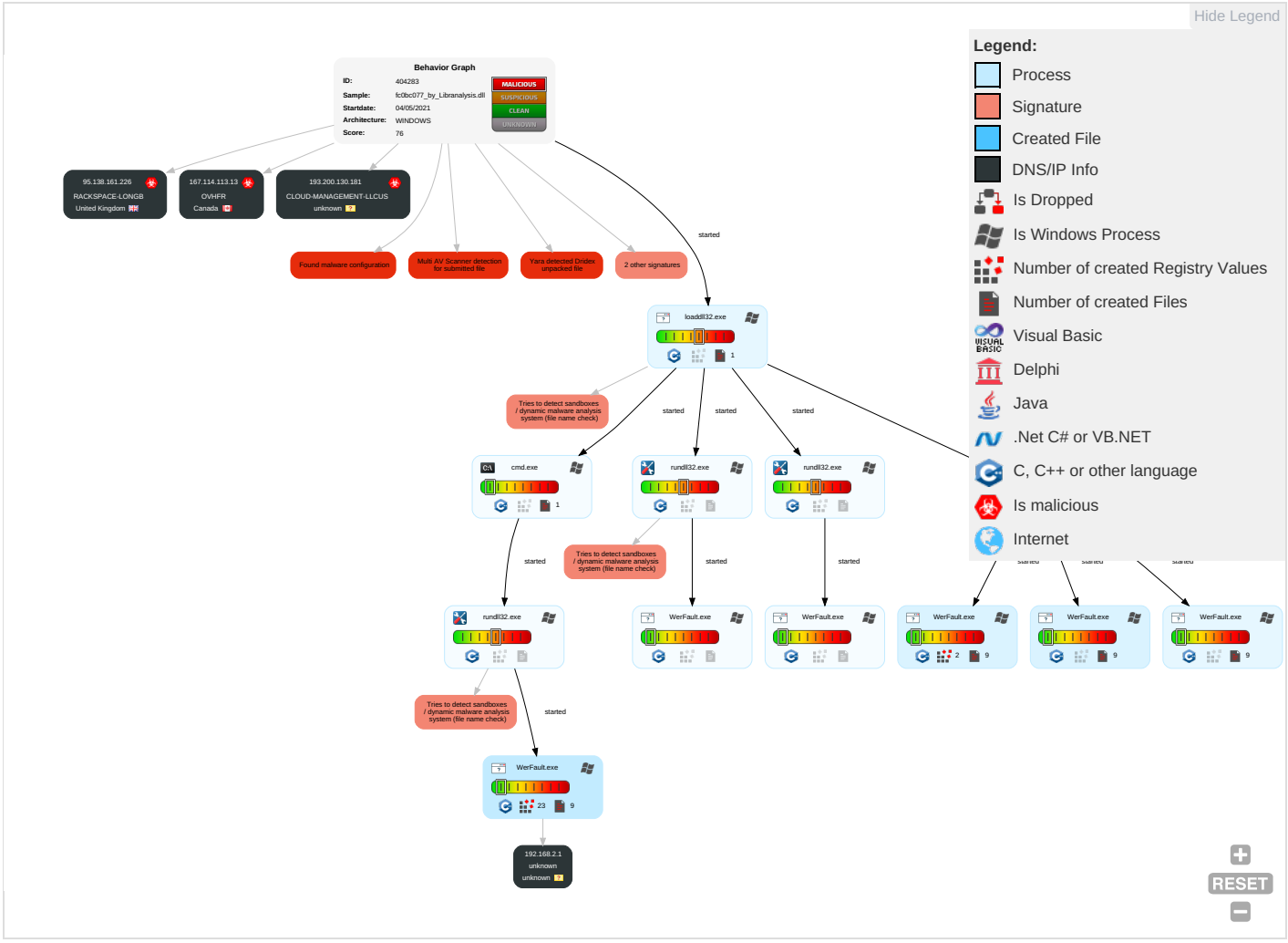
Malware Analysis System Evasion:

Tries to detect sandboxes / dynamic malware analysis system (file name check)

Mitre Att&ck Matrix

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

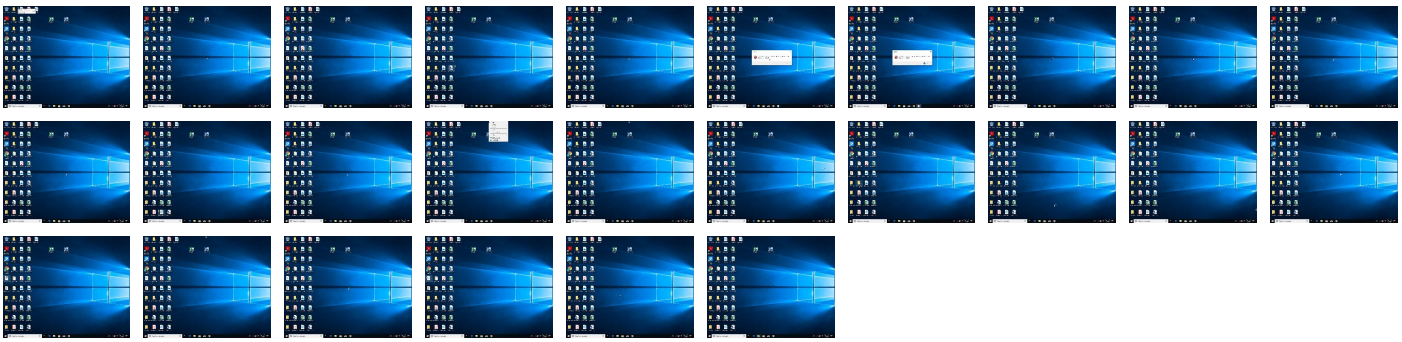
Behavior Graph



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
fc0bc077_by_Libranalysis.dll	21%	Metadefender		Browse
fc0bc077_by_Libranalysis.dll	30%	ReversingLabs	Win32.Trojan.Wacatac	
fc0bc077_by_Libranalysis.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.26c0607.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.1370000.0.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
16.2.rundll32.exe.2920607.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.2cd0000.2.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
18.2.rundll32.exe.2830000.2.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
17.2.rundll32.exe.3200607.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.2d30607.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.2940000.2.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
17.2.rundll32.exe.3220000.2.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
4.2.rundll32.exe.26e0000.2.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.16b0607.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.rundll32.exe.2bc0607.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.rundll32.exe.2810607.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.rundll32.exe.2be0000.2.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
3.2.rundll32.exe.2d50000.2.unpack	100%	Avira	TR/ATRAPS.Gen2		Download File
19.2.rundll32.exe.29e0607.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

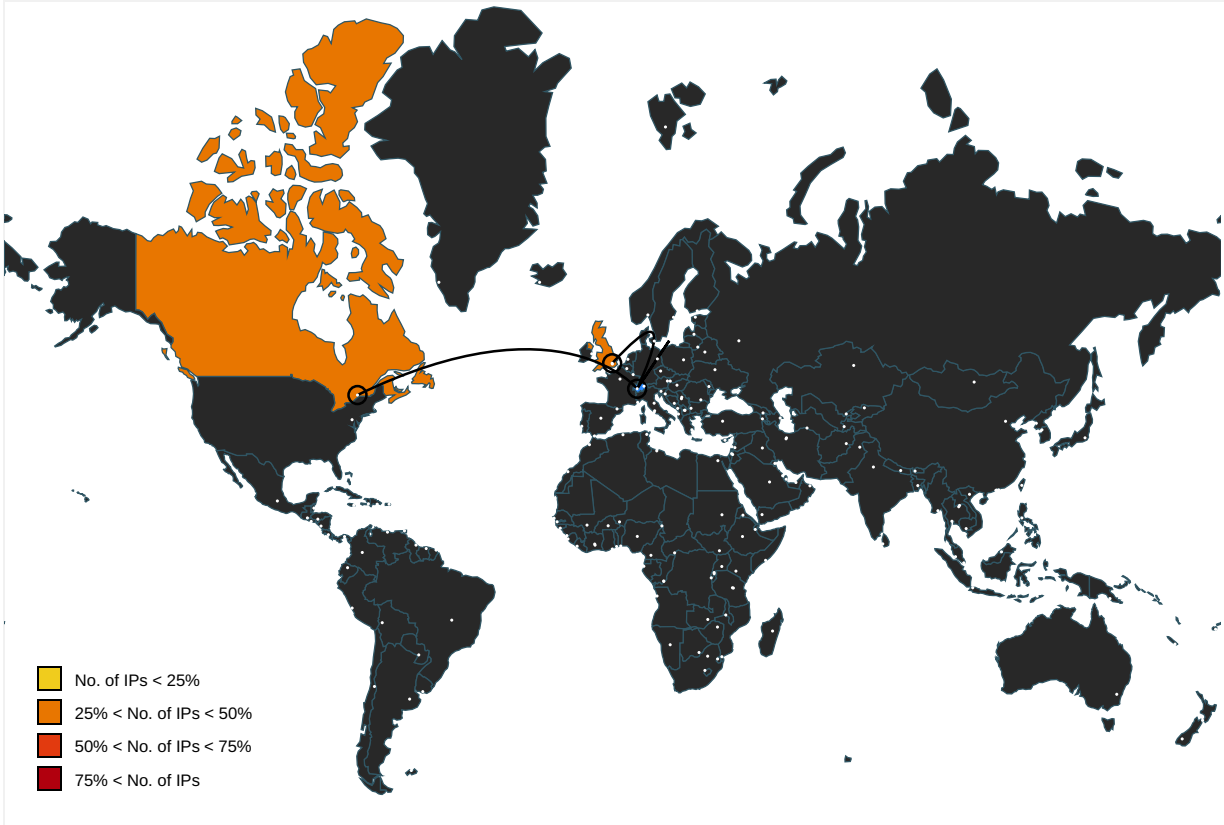
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
167.114.113.13	unknown	Canada		16276	OVHFR	true
95.138.161.226	unknown	United Kingdom		15395	RACKSPACE-LONGB	true
193.200.130.181	unknown	unknown		42960	CLOUD-MANAGEMENT-LLCUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404283
Start date:	04.05.2021
Start time:	21:42:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fc0bc077_by_Libranalysis.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	40
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:	mal76.troj.evad.winDLL@23/24@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 99.2% (good quality ratio 92.6%) • Quality average: 75.3% • Quality standard deviation: 30.5%
HCA Information:	• Successful, ratio: 65% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 13.64.90.137, 184.87.213.153, 104.43.193.48, 23.57.80.111, 2.20.142.209, 2.20.142.210, 40.126.31.4, 40.126.31.1, 20.190.159.136, 20.190.159.134, 40.126.31.8, 40.126.31.143, 40.126.31.135, 40.126.31.6, 40.88.32.150, 52.255.188.83, 20.82.209.104, 92.122.213.247, 92.122.213.194, 20.82.210.154 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, login.live.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
167.114.113.13	577e66d4_by_Libranalysis.dll	Get hash	malicious	Browse	
	b8fe43e6_by_Libranalysis.dll	Get hash	malicious	Browse	
	f845ef61_by_Libranalysis.dll	Get hash	malicious	Browse	
	3c271eae_by_Libranalysis.dll	Get hash	malicious	Browse	
	fc0bc077_by_Libranalysis.dll	Get hash	malicious	Browse	
	e1c88b94_by_Libranalysis.dll	Get hash	malicious	Browse	
	8743016c_by_Libranalysis.dll	Get hash	malicious	Browse	
	d8417415_by_Libranalysis.dll	Get hash	malicious	Browse	
	9a46403f_by_Libranalysis.dll	Get hash	malicious	Browse	
	edae86a8_by_Libranalysis.dll	Get hash	malicious	Browse	
	457aedfd_by_Libranalysis.dll	Get hash	malicious	Browse	
	64b8ed95_by_Libranalysis.dll	Get hash	malicious	Browse	
	8743016c_by_Libranalysis.dll	Get hash	malicious	Browse	
	d8417415_by_Libranalysis.dll	Get hash	malicious	Browse	
	c977c96e_by_Libranalysis.dll	Get hash	malicious	Browse	
	9a46403f_by_Libranalysis.dll	Get hash	malicious	Browse	
	457aedfd_by_Libranalysis.dll	Get hash	malicious	Browse	
	edae86a8_by_Libranalysis.dll	Get hash	malicious	Browse	
	b8dd7ed8_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	af1e75cf_by_Libranalysis.dll	Get hash	malicious	Browse	
95.138.161.226	577e66d4_by_Libranalysis.dll	Get hash	malicious	Browse	
	b8fe43e6_by_Libranalysis.dll	Get hash	malicious	Browse	
	f845ef61_by_Libranalysis.dll	Get hash	malicious	Browse	
	3c271eae_by_Libranalysis.dll	Get hash	malicious	Browse	
	fc0bc077_by_Libranalysis.dll	Get hash	malicious	Browse	
	e1c88b94_by_Libranalysis.dll	Get hash	malicious	Browse	
	8743016c_by_Libranalysis.dll	Get hash	malicious	Browse	
	d8417415_by_Libranalysis.dll	Get hash	malicious	Browse	
	9a46403f_by_Libranalysis.dll	Get hash	malicious	Browse	
	edae86a8_by_Libranalysis.dll	Get hash	malicious	Browse	
	457aedfd_by_Libranalysis.dll	Get hash	malicious	Browse	
	64b8ed95_by_Libranalysis.dll	Get hash	malicious	Browse	
	8743016c_by_Libranalysis.dll	Get hash	malicious	Browse	
	d8417415_by_Libranalysis.dll	Get hash	malicious	Browse	
	c977c96e_by_Libranalysis.dll	Get hash	malicious	Browse	
	9a46403f_by_Libranalysis.dll	Get hash	malicious	Browse	
	457aedfd_by_Libranalysis.dll	Get hash	malicious	Browse	
	edae86a8_by_Libranalysis.dll	Get hash	malicious	Browse	
	b8dd7ed8_by_Libranalysis.dll	Get hash	malicious	Browse	
	af1e75cf_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RACKSPACE-LONGB	577e66d4_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	b8fe43e6_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	f845ef61_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	3c271eae_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	fc0bc077_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	e1c88b94_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	8743016c_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	d8417415_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	9a46403f_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	edae86a8_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	457aedfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	64b8ed95_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	8743016c_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	d8417415_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	c977c96e_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	9a46403f_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	457aedfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	edae86a8_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	b8dd7ed8_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	af1e75cf_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
OVHFR	577e66d4_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	b8fe43e6_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	f845ef61_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	3c271eae_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	fc0bc077_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	e1c88b94_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	8743016c_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	d8417415_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	9a46403f_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	edae86a8_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	457aedfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	64b8ed95_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	8743016c_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	d8417415_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	c977c96e_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9a46403f_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	457aedfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	edae86a8_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	b8dd7ed8_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	af1e75cf_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_0766ec0c\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12698
Entropy (8bit):	3.7729930672976533
Encrypted:	false
SSDEEP:	192:ieiM0oXORH4+V/Ojed+DgR/u7sBS274ItWcq:7iKXOh4+VGjed/u7sBX4ItWcq
MD5:	26D2C96778ACD61D9780C4EBC68E166F
SHA1:	26B7461B9FB449D28ECD6DDE7E99DE8AE63C5BBE
SHA-256:	C4CFF568547C8FEA55F6542B714C6FDBC188903C03D8EAB5B2A35C3103BD095A
SHA-512:	FA9C76A6E32A929A88F3B4DE1055A028A91617829A2F6F72E612A9BA8F857E8DE210406A9A6CB94A5AC04A20DB23BF7F7C257DDA1B5999489954E706A9963101
Malicious:	false
Yara Hits:	• Rule: SUSP_WER_Critical_HeapCorruption, Description: Detects a crashed application that crashed due to a heap corruption error (could be a sign of exploitation), Source: C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_0766ec0c\Report.wer, Author: Florian Roth
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.=.1.3.2.6.4.6.6.3.4.9.2.1.6.6.2.5.7.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.4.6.6.3.4.9.4.5.4.8.1.2.5.7.....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.=.b.6.6.b.e.5.a.1.-.0.1.2.8.-.4.3.3.1.-.b.9.2.b.-.d.e.7.2.b.4.8.0.b.0.3.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.5.d.0.1.1.f.a.-.2.1.a.0.-.4.6.3.c.-.9.6.4.4.-.f.6.7.b.e.7.0.8.f.c.d.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.0.f.f.8.-.0.0.0.1.-.0.0.1.7.-.d.f.9.9.-.0.2.4.8.6.9.4.1.d.7.0.1.....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_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_10f0240f\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12696
Entropy (8bit):	3.774323540979425
Encrypted:	false
SSDEEP:	192:3FiB0oXmRH4+V/Ojed+DgR/u7sQS274ItWc8:VivXmh4+VGjed/u7sQX4ItWc8
MD5:	0C20D6700D4FDF6471A54E7946F4CA18
SHA1:	D963D50A85003F2E41F000D70C816ADDEA69868A
SHA-256:	BD244616AF0012F8328FADB035BEDD3A0514480F6B8B391B3FA59F143DF325E0
SHA-512:	713D98A0AFD2F9DCF28BD48D1328D7477233CE305388615DF42AA8491DE750CE13AF5F8705941975A2CBE40D6D3D092571C45A03A71B2B4A31D6AEEB1262763
Malicious:	false
Yara Hits:	• Rule: SUSP_WER_Critical_HeapCorruption, Description: Detects a crashed application that crashed due to a heap corruption error (could be a sign of exploitation), Source: C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_10f0240f\Report.wer, Author: Florian Roth
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.=.1.3.2.6.4.6.6.3.5.7.1.8.2.9.1.9.0.1.....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.=.1.3.2.6.4.6.6.3.5.7.4.3.7.6.0.5.6.7.....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.b.6.0.5.c.1.b.-.3.9.a.7.-.4.7.d.8.-.a.0.9.9.-.f.b.1.d.9.2.4.5.6.a.8.7.....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.=.0.c.0.1.c.5.a.4.-.8.2.6.5.-.4.e.3.9.-.b.5.1.2.-.2.5.0.5.2.9.a.6.5.8.e.0.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.1.4.3.0.-.0.0.0.1.-.0.0.1.7.-.f.f.b.8.-.1.7.6.5.6.9.4.1.d.7.0.1.....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_70ca6d92bb7cd6d05a398077544511f8e964d76_82810a17_0dc42354\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12770
Entropy (8bit):	3.7728479326199715
Encrypted:	false
SSDEEP:	192:83Prim0oXTHBUZMX4jed+DgR/u7sQS274It7ch:OriAXTBUZMX4jed/u7sQX4It7ch
MD5:	AFC7551E811E97D4890917F0725F1135
SHA1:	ED63C72EE8C1309A591CCF3CDC5A5332F85E6611
SHA-256:	55ACE0B113C0EABD560D6E4668688CD71A30B75590AB9DBAD10CA315AC77A76C
SHA-512:	5392B7C52AF1C27897AA46975DFD75719BD67FDAFA1F38887C623F82E16ADF9D6521493C5A97F1C7FF55A2767F157B3C345DAD95844E42D89AEFDF1B7A5C5B1
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.4.6.6.3.5.7.2.5.9.4.8.1.1.7.....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.=.1.3.2.6.4.6.6.3.5.7.5.0.0.1.0.5.8.9.....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.=.b.a.d.6.9.b.9.f.-.0.8.1.4.-.4.5.9.c.-.a.b.2.3.-.7.1.9.0.c.0.d.1.f.7.7.a.....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.=.3.1.d.d.a.9.6.5.-.0.9.6.e.-.4.3.e.e.-.a.0.7.a.-.5.3.c.e.f.3.4.6.f.2.a.2.....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.=.0.0.0.0.1.2.b.4.-.0.0.0.1.-.0.0.1.7.-.c.5.6.8.-.5.5.6.5.6.9.4.1.d.7.0.1.....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.f.0.9.b.5.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_7dd67966396113c995f4a9c30eeff967a1ce3cd_82810a17_06802046\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12682
Entropy (8bit):	3.769413043333247
Encrypted:	false
SSDEEP:	192:9SVi7K0oXN3xHBUZMX4jed+DoR/u7sQS274ItWcX:QViAXLBUZMX4jeF/u7sQX4ItWcX
MD5:	9440EA7972766E07CD1327E19C1C247B
SHA1:	088A04CA3B6C73A3D7650AB92F6597FFEE89EAF1
SHA-256:	6DEBE33DDFC65B62A5BD2DA29535905133645514D1E48AFC89ECF593E9604E10
SHA-512:	40EEF3E0A6B4115B94C490CA3F0A145F78DC65805BBADAF48B9DC31712F0682E1E8D116EE0908BEEBC3821917C74B67AECA3267F894AF96EA8AD4746380D91E6
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.4.6.6.3.5.7.2.0.6.3.5.6.5.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.4.6.6.3.5.7.4.5.6.3.5.5.7.7.....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.=.5.5.3.0.9.6.9.0.-.8.d.a.1.-.4.5.0.4.-.b.f.3.9.-.e.4.c.a.c.5.7.f.a.d.0.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.9.3.f.0.6.6.7.-.9.f.8.b.-.4.b.a.2.-.a.e.0.a.-.1.0.f.7.5.9.c.e.3.e.9.2.....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.=.0.0.0.0.1.4.4.4.-.0.0.0.1.-.0.0.1.7.-.7.3.b.8.-.a.7.6.5.6.9.4.1.d.7.0.1.....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_85bcb2185548acc57fb6c6745d2f8bb6b2be49b1_82810a17_1454221b\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12680
Entropy (8bit):	3.768900346517595
Encrypted:	false
SSDEEP:	192:IUmix0oX9k3HBUZMX4jed+DgR/u7sQS274ItWcl:jmi/XOBUZMX4jed/u7sQX4ItWcl
MD5:	A12EAA04D0506870309C2F7138A98AA0
SHA1:	9114AE848AE88603BEDDF06398424E3C67DC29D1
SHA-256:	9333B076D9AF6EEBF65B397A53CB3F4BA49336735C8F231FD57A39D8A02369AA
SHA-512:	F18D88FEC310B7F7401FCF5A32931B5D64CBCCEA3200D082774B33EE49C7EB6D3CC38EF3F2C94D292DB2C4B705799A6A03C8E6918CC70C13BD2DFDC8E3C8BAB
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.4.6.6.3.5.7.2.7.3.5.4.3.7.7.....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.=.1.3.2.6.4.6.6.3.5.7.5.0.3.2.3.0.7.8.....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.=.6.0.4.4.b.8.b.2.-.d.d.b.2.-.4.f.0.a.-.b.7.3.a.-.a.0.4.3.a.3.1.8.4.f.6.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.3.7.8.d.a.7.4.-.3.e.6.c.-.4.4.0.6.-.a.4.9.c.-.3.f.b.a.5.5.1.7.4.5.c.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.1.4.5.4.-.0.0.0.1.-.0.0.1.7.-.d.e.8.8.-.1.e.6.6.6.9.4.1.d.7.0.1.....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\ReportQueue\AppCrash_rundll32.exe_868973c6c77b45498eb43d99595a7fe2138962a_82810a17_1682f88f\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_868973c6c77b45498eb43d99595a7fe2138962a_82810a17_1682f88f\Report.wer	
Category:	dropped
Size (bytes):	12856
Entropy (8bit):	3.7590354861574173
Encrypted:	false
SSDEEP:	192:dHip0oX0FHVzOMjed+Do8/u7sBS274It7cp:dHiHXOVzOMje4/u7sBX4It7cp
MD5:	AC6564A38DA01ECB0BE197ACA75CD794
SHA1:	4F9E50FE2F686FE00F5BC846E4ECBB0A54A25B56
SHA-256:	FEFC9EC2AFAB62C5624F71587E383BC844E40ECACD6DFEAEF114ADA2F90EB0D8
SHA-512:	EE4010567180A83E2EEFDCBEB12496BB177EFF8B923195D8B556D66D3ED4039353F07020D140717CB3938DB14BB50DBA109EF1E64A0797FFCB39ACB93723242
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.4.6.6.3.4.9.4.6.5.7.4.9.7.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.5.b.f.2.4.f.9.-.5.5.b.0.-.4.c.8.1.-.8.c.4.1.-.f.5.0.2.7.8.0.3.4.e.1.2.....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.=.a.f.3.e.6.0.0.0.-.4.4.3.b.-.4.1.0.1.-.9.9.4.6.-.4.9.4.1.c.7.2.0.4.2.5.0.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.=.0.0.0.0.1.2.f.c.-.0.0.0.1.-.0.0.1.7.-.2.9.8.8.-.f.a.4.7.6.9.4.1.d.7.0.1.....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.f.0.9.b.5.f.!.r.u.n.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.1.9.8.6././.0.1././.3.0.:.1.1.:.4.2.:.4.4.!.1.0.3.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 5 04:46:13 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	46968
Entropy (8bit):	2.3180308197716517
Encrypted:	false
SSDEEP:	192:iLSUC4DSyUldBW8SqnEaBqAWVbvU2ZHutLribZE5nM7:Py+dI8iuqlbvPYrkUM7
MD5:	FD6A5D857A265F140C64A8EC4401E76E
SHA1:	5BA50E56C090A014951E2CCF09294481C9BBD72F
SHA-256:	35DE6FA92055213621668CADD243C03859D628519623732D27D023B32C2E0E9A
SHA-512:	408CD84742B203FD055FE55327CEC85B87E6AEA73768BFDB67CAD660F724D9CCFC44B802F0E934A05DD105979BD87563D1AD95D377BEA32103ED98EBD773BDB
Malicious:	false
Preview:	MDMP..... .....#.`.....U.....B..... .....GenuineIntelW.....T.....0....".`.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....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\WER11CF.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 5 04:46:13 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	46328
Entropy (8bit):	2.2818682712438516
Encrypted:	false
SSDEEP:	192:5JTH8y+r0xjdDU6zgPCEaBqAWVbvSoDsuNRvt8rWnUa:wy+kd2nuqlbvFTRv6WB
MD5:	89E785F7C61BF264942ABCD23B3CDE58
SHA1:	950214BA1EBBA19EF1A91499F317E00FEAF1E351
SHA-256:	FDD192D0CF9CC7BFDB7F1B06256498FC87F02B6FDE3DCC8E114C6246852EF1B4
SHA-512:	6DFD762243E120D6AC71A5D0FD257AFAE44D74956F146E6443200ABA5B64C9C9341665B5BFD9C69B1E661644295498ED1A96610E09B52E58FC7A03957C9C25E
Malicious:	false
Preview:	MDMP..... .....#.`.....U.....B..... .....GenuineIntelW.....T.....D....".`.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....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\WER13B4.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 5 04:46:14 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	48188
Entropy (8bit):	2.1711333233485948
Encrypted:	false
SSDEEP:	192:vYpWqB8r1dnKLnHH3AY/mGvIoEaBqAWVbvhi2QV9Jx6PnQSKcnv:pqWr7cn3AYOGQ5uqlbvhsJsQSrv
MD5:	128F18CD712C2AE70EBDC763040B46DB

C:\ProgramData\Microsoft\Windows\WER\Temp\WER13B4.tmp.dmp	
SHA1:	3A74DA025DDE09F7299EF3FA65C0C1D890A0B1D4
SHA-256:	D5F9926551CEFB9ABE055F3C985AAE2666881D2FB177332BD9E452FAB62D5C30
SHA-512:	5D17EA7BDEF9F36FD447DBBD49E8C0021C950E02CA5133893A1352A739BFDCFC29D731B87144D94D8BE5FC5328E63FDF91F320574E33AFDE233CC1FE33B3BE 7B
Malicious:	false
Preview:	MDMP..... .....#.`.....U.....B..... .....GenuineIntelW.....T.....".`.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....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\WER1440.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 5 04:46:14 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	39596
Entropy (8bit):	2.4898563574167345
Encrypted:	false
SSDEEP:	192:Cbvk0B1zS7UKocLM/7VrGrt/WQ9M6BMPei:Cw024OCKT99Bcei
MD5:	F61221EE7B709FA21CDE8D6C40CBAE44
SHA1:	AB4EE081228AB2899833E913571709644087B816
SHA-256:	001AA7F47984E90637B69CD29C894A971F7150EC101187527B1FAEECE198163C
SHA-512:	42274DA99FB2828138016888BF6B9DC5ADBD17E92D0023BE7E5A557C55141A8EC5A6CCCD80876BA97560199CAF6CA80918B14F46241F1F59B945783546F54C23
Malicious:	false
Preview:	MDMP..... .....#.`.....U.....B.....P .....GenuineIntelW.....T.....T....".`.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....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\WER181A.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):	8328
Entropy (8bit):	3.7028798362459625
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/d616YBAJ6VC1gmfTHPSXeCpru89bnTsfetm:RrlsNil616YBe6VC1gmfTHPSxn4fV
MD5:	0EF96EFA460D69819DF04855A0C83953
SHA1:	A0896DBDD1F257A071476BD98B8B4C0E69B334D7
SHA-256:	B5B3E798C971E181F0E958A884E2C736EDFD4C9558FF893DA0765B3862CCBFCC
SHA-512:	306822950855FE89F6CD7132AA20BB60A3BEB7892BB39262FD418ED75382274744526F2A5610F9A07018374370A6CD1C8817D4464C8D52F5E20B696ACB4BA90B
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.>.5.1.6.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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):	8314
Entropy (8bit):	3.6953779035389136
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNixG6qE6YBAP6VC1gmfTGGSwCpr+89blzsfhA4m:RrlsNig6B6YBY6VC1gmfTRSPIYf8
MD5:	F75236C3A579EED761F0E10030B6E27A
SHA1:	8A1121F50A9FBA4881EA20F2899CF22872E80479
SHA-256:	0AB3BC6F3164430D89874CED4717C6472E657A13B39B80FBF2C34E1DABF5CCAC
SHA-512:	C5E7213A174DA90E324752406588C9A904F5FFF0ACB11DE815B14F38C9CE3837C933B95EC17EC0A7E50334821D86251783E7A321ABBE7C9D4AF8F53F61F603E9
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	
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.>.5.1.8.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1982.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4679
Entropy (8bit):	4.5104481865614465
Encrypted:	false
SSDEEP:	48:cvIwSD8zstJgtWI9n/WSC8B78fm8M4JCdsrZFydN+q8/3URlv4SrSkd:uITfHUuSNqJpev7DWkd
MD5:	4ABE9138941AF30891290FAE0515DB9B
SHA1:	A83B7E57EB58CE42EC65E383DC579DA7C3ECE6CF
SHA-256:	1E4CF4BE3C12082489172157059442B2615425256D366FBD643170CABAC477D2
SHA-512:	39FF5C1DD408E065ACE7F7CEBBF5CE2671147BDEB7A05D7038B62AA8E64BAC4DBDB7E712AE65D1AC18F1C73FA965D92D45157526E0D3406D45AA652FA9EBE D3E
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="975716" />.. <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\WER1A6C.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4665
Entropy (8bit):	4.475614910572437
Encrypted:	false
SSDEEP:	48:cvIwSD8zstJgtWI9n/WSC8BM8fm8M4JCdskN4xFIwb+q8/9NGnuv4SrS2d:uITfHUuSNXJ2N40mmNGSDW2d
MD5:	4846F50F872E4A8AA53D571CEECD559F
SHA1:	EC8F2D321F6EE4FEE864F21ECE27F9E8CDB1FF99
SHA-256:	8CB133E033F854D6FBE136B2D89A52FB3EEB13F71CBC659B5C83D002FBB255AC
SHA-512:	DD1E51E1A5CA7A22796A9A96EC99C0E17337F91620A6A8C0DC348D4471F4A97821824483C781AE31DA73078691CA20AE9CBD6CA73B8878B31529B7A6B363233
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="975716" />.. <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\WER1A8B.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):	8382
Entropy (8bit):	3.697021584652469
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNimi6Z6YBAT6VC1gmf8eSwCpr189bIFsfC4m:RrlsNi76Z6YBk6VC1gmf8eS6Iefc
MD5:	7EF2060332D0A5610A3207C565CC2D64
SHA1:	BD9CFDCD2D9F6752B026604A60EDCF857EB574C0
SHA-256:	06662A694D2C443D43AE0553CECF3D8781C97A5403024214A993F5EDE548D4FA
SHA-512:	FE5BC54CAE83F064681EC9403C23088F829D9438ED5675DF4226B69D497059732623F3E79C1CA858F028F1DB76CA85A4D42CC19D8E788BD5BAB2AC80F595B82
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.>.4.7.8.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1AE9.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):	8314
Entropy (8bit):	3.6958368096956407
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiVMj6936YBAT6VC1gmfTGsSwCpru89bIWsfIT4m:RrlsNiC6N6YBk6VC1gmfT3SvI1fIZ
MD5:	E13F9F0460180CF911320252CE6CF9C0
SHA1:	1856F05EB0387E3A21BC61D0FF209010AFE0342C
SHA-256:	CFA8BEC43BE69FF45D5DCB11A9F35035D66D0A0C1A4A0FD7E678B6EA0B39C779
SHA-512:	7DA3B9BCA9ACAEDC29CFBBEB511301C9DC9CD9AFA7EC652CE21CF48884782C156A59CF607D52C4096A32D3EE8477E47541C8DF8003868F36B86629453BA79 7B
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.>.5.2.0.4.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BF3.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4770
Entropy (8bit):	4.485189072854489
Encrypted:	false
SSDEEP:	48:cvIwSD8zstJgtWI9n/WSC8BD8fm8M4JCds0MFK+q8vjs0f4SrS5d:uITfHUuSNCJyjKtfDW5d
MD5:	76F4C198B2027A56FDE3377775B02D6A
SHA1:	EB9A75DD8E34CBC8B6FF8C4335490FE33A1C813B
SHA-256:	A979FEE51D81CB7B0F8A16EF2675F414286E0BE4A7CE12C2D22EA6F2BED0D8EA
SHA-512:	F9B64331EFAD0E153309EA056E2B0435AFCDB11C24C067073DB16E1F2600788E0F0E39E291B900E9DC83DBEA0C207E6F4B310724F4D8B446493D9A5F06310EB
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="975716" />.. <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\WER1C42.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4665
Entropy (8bit):	4.47479950329589
Encrypted:	false
SSDEEP:	48:cvIwSD8zstJgtWI9n/WSC8Bb8fm8M4JCdskN4lFi+q8/9NGPGk4SrS6d:uITfHUuSNCJ2N4CmNGtDW6d
MD5:	3134EDDD2FDD88A1D65DB9756C231EB8
SHA1:	7660D8D31893A8C6AAE866B4909CC79928B451F7
SHA-256:	88F009E69E0E5966A9F26A35F46D57A07C92C907F7723946097FE0714C1E8078
SHA-512:	910BAB55C74041FDB6016F9BF7F2F38AAE0A4F2EA2EB70E68BBE2969363BC2E3EE3052AAA376E6CC3527031A8DB11465DEF8EB40A72E0FB7055D6BB892DCCF 48
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="975716" />.. <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\WERD97E.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 5 04:44:53 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	46648
Entropy (8bit):	2.4535395835887615

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	
Encrypted:	false
SSDEEP:	192:9umavpqvZkOvC3hcnoZofEaBqAWVbvx2p5R+6J86cndbpU:ivMRd67ruqlbvQJJ2DU
MD5:	7AE3527170E540035BDD93E0EE31C096
SHA1:	14A3BA01D791E538CDF6845415F8D025C89C4931
SHA-256:	A31507D3C30BE23DCC3FD2163DAC1DDD8A885372CDA1371D70155DE170E41007
SHA-512:	4C9E6C15030CE194524D6806935938F0194CBA2CB0C41D1A29EE6B3AED10DBB93FB84853C3463DB20F15269390B1E93F55F5F9E802C6E8FC5E24737E08DA687
Malicious:	false
Preview:	MDMP..... .....".`.....U.....B..... .....GenuineIntelW.....T.....".`.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....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\WERE0E2.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):	8308
Entropy (8bit):	3.702193352850464
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiJP6P6YBVq62lgmfTHPSXeCprN89bOQsf5am:RrlsNiB6P6YBo62lgmfTHPScOjfF
MD5:	5B80932A4AC95EB65E3ACA9DDA87E718
SHA1:	9B9BE79028FC60FFDC206B5D68ABBAEF95FD33ED
SHA-256:	D65FC1C0C6358462EB3491E6D175B3C590390198D602F9DE58A29DAE9B84F815
SHA-512:	AFBDFAB58086D61B8745AA988629588E08E93DAF3F98771AB9EB02BFDCF64A2AA2381B166407BED1DBAFCCE10B0AD8DF401AC81371E72CAFA0D96072073A91D4
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.>.4.0.8.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1AE.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4679
Entropy (8bit):	4.510648672121708
Encrypted:	false
SSDEEP:	48:cvIwSD8zsEJgtWI9n/WSC8BY8fm8M4JCdsrZFE+q8/3UM4SrSH1d:uITfCUuSNTJpovMDWH1d
MD5:	3D916DD79CDE1C883423BD9B839B953F
SHA1:	62CA53FF330706120B5519B143FCEC7BD6DB4247
SHA-256:	681344A6C49F9419C18BD31836A0B7D655253DE18874C3B9AE80054B0E2CE14D
SHA-512:	A97E39D45F37CA5D0EDD5854C1442002588F8C17923BC63537C92D0A41E06208A81BFCB0B760003E16822B918046947B4026EF01DD7BF70EFC01B8070386D2F0
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="975715" />.. <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\WERE342.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed May 5 04:44:57 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	55668
Entropy (8bit):	2.2904308539354665
Encrypted:	false
SSDEEP:	192:y+zeWh19dnkac2JDEj1aI/980h3AMCCcDqiSP3FjYZdIhZ0ynImBo2uPzhcB:pzeWldFcC0w6mGCE5P5YZi9XxubyB
MD5:	E34E085293DC18A24A3DDC8F35287D65
SHA1:	28270F46B36994AC7DF344FEFAB8642DE830AB19
SHA-256:	7BB4A909167FB906A87CDE2A234E95186ABD940C21F9BFA7844C38AF1B2B02FF
SHA-512:	682AFA5F0552E934EC6E8FC90607E02354376166296FE80E9C35004F2721BB6F45F34469316F9EF0AA5A3A26C9D35073EDB092883A62C9AEE6BD6AE1CB0F7C19

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	
Malicious:	false
Preview:	MDMP..... .....".`.....U.....B....."......GenuineIntelW.....T....."."`.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....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\WERF66D.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):	8380
Entropy (8bit):	3.6919968957861586
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNind606YBAV6L6Cdgmf8GHS7CpBg89b7XsfFpm:RrlsNid606YB66WCdgmf8USM7cfC
MD5:	4D4A7E4D09FAA799E97D6176C63AE803
SHA1:	E0BC1FD43A1BF867A6102731AAEEFDB0A7FE95D8
SHA-256:	FE002D89650D220CD275724E3C7982D0B82FA48C3DA934A67DA7CF5F00C36815
SHA-512:	4DB6A8811591527BEA21D2AB760DFD25405436599894AA0920D4E04F8D888113C5202A293C3FDFA09B1D0E3F196CBC4933E0F1DE7ADA46468213282E9C9259A5
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.>.4.8.6.0.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF833.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4766
Entropy (8bit):	4.458276862803724
Encrypted:	false
SSDEEP:	48:cvIwSD8zsEJgtWI9n/WSC8Bh8fm8M4JCdskN4fFApF+q8vjskN4T4SrSCd:uITfCUuSNsJ2N4KfKrN4TDWCd
MD5:	0A2B816991697FE1C620267C2B0C607A
SHA1:	9A1F08BA075938CADB65A79F3ADD7F34875D86B5
SHA-256:	BF2E2E4527DC9096AAF9EE9856E38D289EDFF1F72CE97F6E55B9E7B03DED5413
SHA-512:	2DB64775768B9E633663A98263550F1583C0D72257FAE05A7AB34E56FEB9237B903C5731B9714C431026FE5AFCEDDC9DF2025E39C5348F3A6D7E8964D6D4A3FD
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="975715" />.. <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):	7.53604314211802
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:	fc0bc077_by_Libranalysis.dll
File size:	164864
MD5:	fc0bc07721ce94bc9b100e7c846a1210
SHA1:	2d98f05fb78cd75bb44a0087bead8c1604545d07
SHA256:	e707edac036a1a2d08b746c6a50ac0f0e2b1ba1c2668aadf87ea11b666b0eb28

General

SHA512:	148d0dbd3b2cfa7a9182f073e13a83bbbf5cbce934b04366b539799007df341bf953308647f0bee16e351b3716f25e4e10c349dfda5bae70ded3cae208621b35
SSDEEP:	3072:sC2X+QFg3UutDvUvoU8pz6EJEEhu6Tzace9kuaGA81/YXKHML/Vp8AF:MG3rUvoU4JE/Wzan9T7B/CKsL/Vy
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t.%.0zK.0zK.0zK.0zJ.}{K...3..{K.....P{K...3..zK.V....zK...1..{K.....zK.Rich0zK.....PE..L..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100241a0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60903ADD [Mon May 3 18:03:09 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	f108efab351dd21acb187c36805c5bbe

Entrypoint Preview

Instruction
mov edx, eax
xor eax, eax
add eax, 00002233h
cmpss xmm1, xmm2, 03h
sub eax, 00002233h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
cmp eax, 01h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

Instruction
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

Rich Headers

Programming Language:	• [RES] VS2012 UPD3 build 60610 • [LNK] VS2005 build 50727 • [EXP] VS2005 build 50727 • [C] VS2012 UPD4 build 61030 • [IMP] VS2013 UPD2 build 30501

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x27730	0x55	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x27804	0x59	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x3a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2d000	0x1220	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x10018	0x38	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x25000	0x60	.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	0x23322	0x23400	False	0.759010693706	data	7.5511794748	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2e39	0x2c00	False	0.770774147727	data	7.47865520081	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pdata	0x28000	0x336c	0x1800	False	0.78564453125	MMDF mailbox	7.42299069747	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x48c	0x400	False	0.4091796875	data	3.06807977608	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0x258	0x400	False	0.5263671875	data	4.16057022331	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x2c060	0x33c	data		

Imports

DLL	Import
msvcrt.dll	memset
ADVAPI32.dll	RegOverridePredefKey
ole32.dll	CreatePointerMoniker, CreateStreamOnHGlobal
USER32.dll	TranslateMessage
OPENGL32.dll	glTexSubImage1D
KERNEL32.dll	CloseHandle, OutputDebugStringA, LoadLibraryExW, CreateFileW, GetProfileSectionW, LoadLibraryW, GetProfileSectionA, OpenSemaphoreW
RASAPI32.dll	RasGetConnectionStatistics
CLUSAPI.dll	ClusterEnum

Exports

Name	Ordinal	Address
LoxmtYt	1	0x10027776

Version Infos

Description	Data
LegalCopyright	Copyright 2018
InternalName	j2pcsc
FileVersion	8.0.1710.11
Full Version	1.8.0_171-b11
CompanyName	Oracle Corporation
ProductName	Java(TM) Platform SE 8
ProductVersion	8.0.1710.11
FileDescription	Java(TM) Platform SE binary
OriginalFilename	j2pcsc.dll
Translation	0x0000 0x04b0

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:43:07.290054083 CEST	50620	53	192.168.2.3	8.8.8.8
May 4, 2021 21:43:07.340730906 CEST	53	50620	8.8.8.8	192.168.2.3
May 4, 2021 21:43:08.356738091 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 21:43:08.410634995 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 21:43:08.711296082 CEST	60152	53	192.168.2.3	8.8.8.8
May 4, 2021 21:43:08.771044970 CEST	53	60152	8.8.8.8	192.168.2.3
May 4, 2021 21:43:09.556556940 CEST	57544	53	192.168.2.3	8.8.8.8
May 4, 2021 21:43:09.621206999 CEST	53	57544	8.8.8.8	192.168.2.3
May 4, 2021 21:43:10.489531994 CEST	55984	53	192.168.2.3	8.8.8.8
May 4, 2021 21:43:10.539915085 CEST	53	55984	8.8.8.8	192.168.2.3
May 4, 2021 21:43:11.973864079 CEST	64185	53	192.168.2.3	8.8.8.8
May 4, 2021 21:43:12.027225018 CEST	53	64185	8.8.8.8	192.168.2.3
May 4, 2021 21:43:13.452745914 CEST	65110	53	192.168.2.3	8.8.8.8
May 4, 2021 21:43:13.501549006 CEST	53	65110	8.8.8.8	192.168.2.3
May 4, 2021 21:43:14.552916050 CEST	58361	53	192.168.2.3	8.8.8.8
May 4, 2021 21:43:14.602003098 CEST	53	58361	8.8.8.8	192.168.2.3
May 4, 2021 21:43:15.522281885 CEST	63492	53	192.168.2.3	8.8.8.8
May 4, 2021 21:43:15.570959091 CEST	53	63492	8.8.8.8	192.168.2.3
May 4, 2021 21:43:45.853096008 CEST	60831	53	192.168.2.3	8.8.8.8
May 4, 2021 21:43:45.936233997 CEST	53	60831	8.8.8.8	192.168.2.3
May 4, 2021 21:43:58.366470098 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 21:43:58.420455933 CEST	53	60100	8.8.8.8	192.168.2.3
May 4, 2021 21:43:59.903868914 CEST	53195	53	192.168.2.3	8.8.8.8
May 4, 2021 21:43:59.963656902 CEST	53	53195	8.8.8.8	192.168.2.3
May 4, 2021 21:44:01.529102087 CEST	50141	53	192.168.2.3	8.8.8.8
May 4, 2021 21:44:01.580902100 CEST	53	50141	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:44:01.986046076 CEST	53023	53	192.168.2.3	8.8.8.8
May 4, 2021 21:44:02.046535969 CEST	53	53023	8.8.8.8	192.168.2.3
May 4, 2021 21:44:04.101972103 CEST	49563	53	192.168.2.3	8.8.8.8
May 4, 2021 21:44:04.158121109 CEST	53	49563	8.8.8.8	192.168.2.3
May 4, 2021 21:45:20.032542944 CEST	51352	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:20.107333899 CEST	59349	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:20.127286911 CEST	53	51352	8.8.8.8	192.168.2.3
May 4, 2021 21:45:20.158092022 CEST	53	59349	8.8.8.8	192.168.2.3
May 4, 2021 21:45:20.577899933 CEST	57084	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:20.637445927 CEST	53	57084	8.8.8.8	192.168.2.3
May 4, 2021 21:45:21.121624947 CEST	58823	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:21.155797958 CEST	57568	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:21.170548916 CEST	53	58823	8.8.8.8	192.168.2.3
May 4, 2021 21:45:21.214432001 CEST	53	57568	8.8.8.8	192.168.2.3
May 4, 2021 21:45:21.667354107 CEST	50540	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:21.725111961 CEST	53	50540	8.8.8.8	192.168.2.3
May 4, 2021 21:45:22.202001095 CEST	54366	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:22.208492994 CEST	53034	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:22.250680923 CEST	53	54366	8.8.8.8	192.168.2.3
May 4, 2021 21:45:22.260543108 CEST	53	53034	8.8.8.8	192.168.2.3
May 4, 2021 21:45:23.365561008 CEST	57762	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:23.380847931 CEST	55435	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:23.429649115 CEST	53	55435	8.8.8.8	192.168.2.3
May 4, 2021 21:45:23.430177927 CEST	53	57762	8.8.8.8	192.168.2.3
May 4, 2021 21:45:23.492109060 CEST	50713	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:23.549302101 CEST	53	50713	8.8.8.8	192.168.2.3
May 4, 2021 21:45:23.920649052 CEST	56132	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:23.966571093 CEST	58987	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:23.981606007 CEST	53	56132	8.8.8.8	192.168.2.3
May 4, 2021 21:45:24.023734093 CEST	53	58987	8.8.8.8	192.168.2.3
May 4, 2021 21:45:24.175579071 CEST	56579	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:24.226135015 CEST	53	56579	8.8.8.8	192.168.2.3
May 4, 2021 21:45:24.973644972 CEST	60633	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:25.030881882 CEST	53	60633	8.8.8.8	192.168.2.3
May 4, 2021 21:45:25.818038940 CEST	61292	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:25.878962040 CEST	53	61292	8.8.8.8	192.168.2.3
May 4, 2021 21:45:26.423403978 CEST	63619	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:26.480717897 CEST	53	63619	8.8.8.8	192.168.2.3
May 4, 2021 21:45:27.331106901 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 21:45:27.382663965 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 21:46:02.031594992 CEST	61946	53	192.168.2.3	8.8.8.8
May 4, 2021 21:46:02.091624975 CEST	53	61946	8.8.8.8	192.168.2.3
May 4, 2021 21:46:09.996799946 CEST	64910	53	192.168.2.3	8.8.8.8
May 4, 2021 21:46:10.050515890 CEST	53	64910	8.8.8.8	192.168.2.3
May 4, 2021 21:46:22.169416904 CEST	52123	53	192.168.2.3	8.8.8.8
May 4, 2021 21:46:22.219254971 CEST	53	52123	8.8.8.8	192.168.2.3

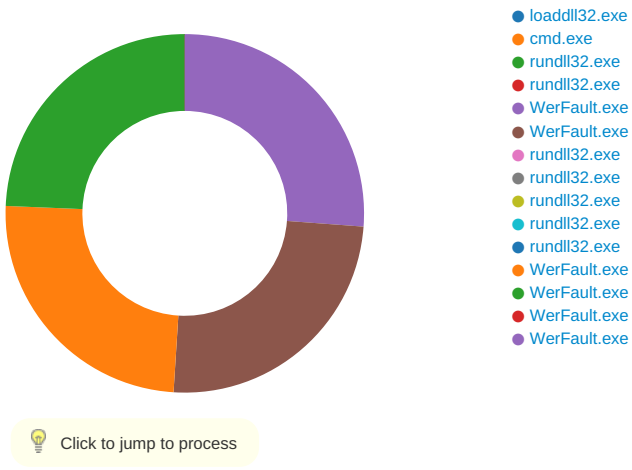
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:45:20.127286911 CEST	8.8.8.8	192.168.2.3	0x80ed	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:45:20.637445927 CEST	8.8.8.8	192.168.2.3	0xe98c	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:45:21.214432001 CEST	8.8.8.8	192.168.2.3	0x72fd	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:45:21.725111961 CEST	8.8.8.8	192.168.2.3	0x16d1	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:45:26.480717897 CEST	8.8.8.8	192.168.2.3	0x568	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 5980 Parent PID: 5684

General

Start time:	21:44:06
Start date:	04/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll'
Imagebase:	0x190000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 5984 Parent PID: 5980

General

Start time:	21:44:06
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',#1
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 4860 Parent PID: 5980

General

Start time:	21:44:06
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll,LoxmtYt
Imagebase:	0x1c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 4088 Parent PID: 5984

General

Start time:	21:44:06
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',#1
Imagebase:	0x1c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000004.00000002.326004095.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 1848 Parent PID: 4088

General

Start time:	21:44:50
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4088 -s 760
Imagebase:	0xa80000
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	702B1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1AE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1AE.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_0766ec0c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_0766ec0c\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	702A497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1AE.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1AE.tmp.xml	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36D7.tmp.csv	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36F7.tmp.txt	success or wait	1	702A4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 c5 22 92 60 a4 05 12 00 00 00 00 00	MDMP........ ....".`........	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.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 80 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 f8 0f 00 00 96 22 92 60 07 00 00 00 12 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 3d 00 00 00 00 00 00 00 02 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 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....... .... ..GenuineIntelW...........T... ....".`.................. ....0..=............... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e................... ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.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 80 02 02 00 00 00 c0 58 f0 77 90 58 f0 77 01 00 00 00 84 f7 63 02 f4 f7 63 02 79 8e ec 77 23 00 00 00 46 02 00 00 60 f7 63 02 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...+. ..+............X.w.X.w......c. ..c.y..w#...F...`.c.+.........	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	unknown	168	fc 0f 00 00 00 00 00 00 74 03 00 c0 01 00 00 00 00 00 00 00 00 00 00 00 79 8e ec 77 00 00 00 00 01 00 00 00 00 00 00 00 90 58 f0 77 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 cc f7 63 02 00 00 00 00 00 64 02 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 88 f7 63 02 00 00 00 00 00 00 00 00 00 00 00 00 24 f8 63 02 00 00 00 00 f0 17 e6 77 00 00 00 00 b0 3f f7 bc ff ff ff ff fe ff ff ff ff ff ff f0 f7 63 02 00 00 00 00 d1 86 e4 77 00 00 00 00 cc 02 00 00 8a 26 00 00	........t.....y..w.. ....X.w..... ......c.....d..... ....c.....$.c..... ...w.....?.....c... .....w.....&..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	unknown	20	10 00 00 00 f9 8d ec 77 00 00 00 00 00 01 00 00 be 32 00 00	.......w.....2..	success or wait	16	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	unknown	256	eb 42 fa ff 89 55 84 89 4d 8c 64 a1 30 00 00 00 8a 40 02 84 c0 75 10 a0 d4 02 fe 7f 24 03 3c 03 0f 94 c0 84 c0 74 2d 51 68 c8 da e0 77 6a 00 6a 65 e8 f1 c8 fd ff 83 c4 10 83 7d 08 00 74 15 83 65 fc 00 cc eb 07 33 c0 40 c3 8b 65 e8 c7 45 fc fe ff ff 33 c9 41 89 4d fc 8b 45 8c 89 45 90 89 4d 94 83 65 98 00 c7 45 9c f0 de e6 77 89 4d a0 8b 45 84 89 45 a4 8d 45 90 50 e8 77 50 fa ff eb 36 8b 4d ec 8b 01 8b 00 89 85 7c ff ff ff 89 4d 88 89 45 80 6a 00 8b 45 88 ff 70 04 8b 45 88 ff 30 e8 90 7d fd ff ff 75 80 6a ff e8 16 09 f9 ff 33 c0 40 c3 8b 65 e8 c7 45 fc fe ff ff ff e8 73 42 fa ff c2 04 00 8b ff 55 8b ec 51 0f b7 01 66 85 c0 74 2d 8b 51 04 d1 e8 8d 4a fe 8d 0c 41 eb 1c 0f b7 01 83 f8 5c 74 18 83 f8 40 73 0c 0f b6 80 f0 da e0 77 83 e0 08 75 0d 83 e9 02 3b	.B...U..M.d.0....@...u.....$. <.....t-Qh...wj.je.....}. .t..e.....3.@..e..E.....3.A.M. .E..E..M..e...E....w.M..E..E. .E.P.wP...6.M.....|....M..E.j ..E..p..E..0..}...u.j.....3.@ ..e..E.....sB.....U..Q...f..t- .Q....J...A.....\t...@s.. .....w...u....;	success or wait	15	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	unknown	4096	dc fd 26 04 00 00 27 04 00 40 26 04 00 00 00 00 00 1e 00 00 00 00 00 00 00 c0 59 02 00 00 00 00 f8 0f 00 00 e0 0b 00 00 00 00 00 00 00 00 00 00 00 00 d0 58 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00	..&...'..@&...............Y... ....X......... ....p.w.............	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.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 00 00 00 00 00 00 00 00 90 58 f0 77 aa aa aa aa 00 00 00 00 d8 e9 63 02 bc 9a e5 77 23 00 00 00 02 02 00 00 98 e9 63 02 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...+. ..+................X.w........ ..c....w#.........c.+.........	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	unknown	48	e0 0b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 c0 59 02 00 00 00 00 00 30 fc 26 04 00 00 00 00 d0 03 00 00 be 33 00 00 cc 02 00 00 ee 2e 00 00	....Y.....0.&... ....3..........	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	unknown	4	35 00 00 00	5...	success or wait	53	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.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	53	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	unknown	752	00 00 48 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 70 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 e0 8e 02 00 00 00 00 00 80 de 02 00 00 00 00 48 54 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 b2 6b 03 00 00 00 00 00 b7 6b 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5f 8e 15 00 00 00 00 00 e1 70 0a 00 00 00 00 00 40 ff 1f 00 00 00 00 00 52 84 0a 00 00 00 00	..Ht.....0...U..s@..p&.....B.....B?.....#.....@A.....Zb.....HT.....k.....k....._.....p.....@.....R.....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	unknown	10774	12 00 00 00 44 00 69 00 72 00 65 00 63 00 74 00 6f 00 72 00 79 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 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	....D.i.r.e.c.t.o.r.y.....F.i.l.e.....F.i.l.e.....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	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD97E.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 60 16 00 00 9c 07 00 00 05 00 00 00 04 01 00 00 ba 31 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 38 1e 00 00 48 98 00 00 15 00 00 00 ec 01 00 00 fc 1d 00 00 16 00 00 00 98 00 00 00 e8 1f 00 00	..... ` ... 1 ..... T ..... 8 .... T ..... 8 ... H	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 30 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.0.8.8.<./.P.i.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 37 00 34 00 32 00 36 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.>.4.7.4.2.6.<./.U.p.t.i.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 32 00 38 00 38 00 33 00 39 00 36 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.8.3.9.6.8.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 32 00 38 00 38 00 33 00 31 00 34 00 38 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.8.3.1.4.8.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 36 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.6.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 34 00 30 00 38 00 35 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.4.0.8.5.1.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 34 00 30 00 38 00 35 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.4.0.8.5.1.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 38 00 36 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 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.>.1.8.6.8.8.0.<./.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 36 00 36 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.6.6.8.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 33 00 31 00 38 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.3.1.8.0.8.<./.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 33 00 31 00 35 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.1.5.3.6.<./.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 35 00 39 00 39 00 36 00 35 00 34 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.>.5.9.9.6.5.4.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 36 00 30 00 30 00 34 00 37 00 33 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.>.6.0.0.4.7.3.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 35 00 39 00 39 00 36 00 35 00 34 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.>.5.9.9.6.5.4.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.9.8.4.<./.P.i.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 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.>.c.m.d...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 37 00 37 00 39 00 33 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.>.4.7.7.9.3. <./.U.p.t.i.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.5.7.4.0.5.4.4.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 35 00 32 00 31 00 32 00 39 00 37 00 39 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.>.5.2.1.2.9.7.9.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 31 00 32 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.2.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 33 00 37 00 31 00 35 00 30 00 37 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.>.3.7.1.5.0.7.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 33 00 36 00 37 00 38 00 32 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.>.3.6.7.8.2.0.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 39 00 36 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 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.>.4.0.9.6.0.<./.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 32 00 31 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.>.3.3.2.1.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.5.6.3.2.<./.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 39 00 35 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.>.4.9.5.2.<./.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 32 00 34 00 36 00 31 00 36 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.4.6.1.6.9.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 35 00 37 00 31 00 37 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.7.1.7.1.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 32 00 34 00 36 00 31 00 36 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.4.6.1.6.9.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 73 00 77 00 71 00 75 00 73 00 73 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.>.s.w.q.u.s.s.,. .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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 73 00 77 00 71 00 75 00 73 00 73 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.>.s.w.q.u.s.s.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 36 00 32 00 30 00 38 00 31 00 34 00 35 00 39 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.2.0.8.1.4.5.9.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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.>.0.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 35 00 2d 00 30 00 35 00 54 00 30 00 34 00 3a 00 34 00 34 00 3a 00 35 00 34 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.-.0.5.-.0.5.T.0.4.:.4.4.:.5.4.Z.".>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	266	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 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 30 00 38 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 32 00 35 00 31 00 35 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 32 00 35 00 31 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.4.3.". .P.I.D.=.".4.0.8.8.". .U.p.t.i.m.e.M.S.=.".4.2.5.1.5.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".4.2.5.1.5.". .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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 36 00 36 00 62 00 65 00 35 00 61 00 31 00 2d 00 30 00 31 00 32 00 38 00 2d 00 34 00 33 00 33 00 31 00 2d 00 62 00 39 00 32 00 62 00 2d 00 64 00 65 00 37 00 32 00 62 00 34 00 38 00 30 00 62 00 30 00 33 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.b.6.6.b.e.5.a.1.-.0.1.2.8.-.4.3.3.1.-.b.9.2.b.-.d.e.7.2.b.4.8.0.b.0.3.4.<./.G.u.i.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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 35 00 2d 00 30 00 35 00 54 00 30 00 34 00 3a 00 34 00 34 00 3a 00 35 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.0.5.T.0.4.:.4.4.:.5.4.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E2.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	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE1AE.tmp.xml	unknown	4679	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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_0766ec0c\Report.wer	unknown	2	ff fe	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_0766ec0c\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	184	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_0766ec0c\Report.wer	unknown	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 37 00 33 00 32 00 31 00 30 00 39 00 37 00 34 00 32 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.7.3.2.1.0.9.7.4.2.	success or wait	1	702A497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	702C36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	702C1FB2	RegCreateKeyExW
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702A43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	702C36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	702C36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	74 03 00 C0 01 00 00 00 00 00 00 00 79 8E EC 77 01 00 00 00 90 58 F0 77 00 00 00 00 0A 00 00 00 CC F7 63 02 00 00 64 02 00 00 00 00 0A 00 00 00 88 F7 63 02 00 00 00 00 24 F8 63 02 F0 17 E6 77 B0 3F F7 BC FE FF FF FF F0 F7 63 02 D1 86 E4 77	success or wait	1	702C1FE8	RegSetValueExW

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

Analysis Process: WerFault.exe PID: 5852 Parent PID: 4860

General

Start time:	21:44:53
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4860 -s 788
Imagebase:	0xa80000
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	702B1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF833.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF833.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_868973c6c77b45498eb43d99595a7fe2138962a_82810a17_1682f88f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_868973c6c77b45498eb43d99595a7fe2138962a_82810a17_1682f88f\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	702A497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF833.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF833.tmp.xml	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D6E.tmp.csv	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4D9E.tmp.txt	success or wait	1	702A497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 c9 22 92 60 a4 05 12 00 00 00 00 00	MDMP..... ....."."`.....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.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 fc 22 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 12 00 00 96 22 92 60 08 00 00 00 12 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 3d 00 00 00 00 00 00 00 02 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 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	.....U...........B.......".... ..GenuineIntelW..........T... ....".`................. ....0..=.............. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.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 10 f0 f9 9a 02 00 00 00 00 ff ff ff ff 00 00 00 10 00 00 00 00 fc f9 9a 02 00 00 00 10 23 00 00 00 46 02 01 00 e0 f9 9a 02 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...+. ..+........................... ....#...F.......+.........	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	unknown	168	ec 02 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 06 2a 00 00	....*..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	unknown	20	17 00 00 00 04 fd 80 04 00 00 00 00 fc 02 00 00 76 39 00 00	...............v9..	success or wait	23	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	unknown	764	bc b1 e5 77 d6 c9 e3 77 50 00 00 00 aa aa aa aa 10 00 00 00 98 fd 80 04 64 fe 80 04 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa aa aa aa aa 00 00 00 00 78 07 d8 02 50 00 00 00 aa aa aa aa 50 00 00 00 aa aa aa aa aa aa aa aa 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 aa aa aa aa 60 05 d9 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 a7 02 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 c8 f8 fd 05 54 12 a7 02 e8 07 d8 02 e8 07 d8 02 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	...w...wP...............d.......@..w@..w............x...P.......P..`...T..	success or wait	22	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	unknown	256	c2 10 00 90 b8 c4 01 00 00 ba e0 dc e6 77 ff d2 c2 0c 00 90 b8 c5 01 00 00 ba e0 dc e6 77 ff d2 c2 04 00 90 b8 c6 01 00 00 ba e0 dc e6 77 ff d2 c2 1c 00 90 b8 c7 01 00 00 ba e0 dc e6 77 ff d2 c2 08 00 90 b8 c8 01 06 00 ba e0 dc e6 77 ff d2 c2 08 00 90 b8 c9 01 00 00 ba e0 dc e6 77 ff d2 c2 10 00 90 b8 ca 01 15 00 ba e0 dc e6 77 ff d2 c2 10 00 90 b8 cb 01 00 00 ba e0 dc e6 77 ff d2 c2 14 00 90 b8 cc 01 03 00 ba e0 dc e6 77 ff d2 c2 04 00 90 b8 cd 01 03 00 ba e0 dc e6 77 ff d2 c2 04 00 90 b8 ce 01 00 00 ba e0 dc e6 77 ff d2 c2 14 00 90 b8 cf 01 00 00 ba e0 dc e6 77 ff d2 c3 8d 49 00 b8 d0 01 00 00 ba e0 dc e6 77 ff d2 c2 10 00 90 b8 d1 01 00 00 ba e0 dc e6 77 ff d2 c2 08 00 90 b8 d2 01 00 00 ba e0 dc e6 77 ff d2 c2 04 00 90 b8 d3 01 00 00 ba e0 dc e6 77 ff	............w..............w ....w............. .w..............w........... ...w..............w......... .....w..............w....... ....w..............w...... ....w....I..........w.... ....w..............w.. ....w.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.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 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 10 00 00 00 00 48 ec 9a 02 bc 9a e5 77 23 00 00 00 02 02 00 00 08 ec 9a 02 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...+. ..+........................... H......w#...........+.........	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	unknown	48	50 0c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 60 a8 02 00 00 00 00 58 f9 05 06 00 00 00 00 a8 06 00 00 b6 9d 00 00 cc 02 00 00 36 35 00 00	P....... ....`......X..... ....65..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	unknown	4	3a 00 00 00	:...	success or wait	58	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.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	58	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	unknown	120	00 00 c3 6f 00 00 00 00 00 60 0d 00 20 d1 0d 00 aa 0c c7 bd aa 29 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 00 25 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 0c 00 00 00 18 00 00 00 01 00 00 00	...o.....`.. ....)..... .....B.....B?..... .....%..... ..@A.....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	unknown	62	38 00 00 00 66 00 63 00 30 00 62 00 63 00 30 00 37 00 37 00 5f 00 62 00 79 00 5f 00 4c 00 69 00 62 00 72 00 61 00 6e 00 61 00 6c 00 79 00 73 00 69 00 73 00 2e 00 64 00 6c 00 6c 00 00 00	8...f.c.0.b.c.0.7.7._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...d.l.l...	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	unknown	668	00 00 00 10 00 00 00 00 00 10 02 00 00 00 00 00 3b cc 7e 60 c8 29 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 c0 7d 02 00 00 00 00 00 80 de 02 00 00 00 00 d7 54 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 89 71 03 00 00 00 00 00 89 71 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 99 7e 15 00 00 00 00 00 a7 80 0a 00 00 00 00 00 40 ff 1f 00 00 00 00 00 04 97 0a 00 00 00 00 00 6e d9 a2 42 00 00 00 00 af a7 83 15 00 00 00 00 a8 ab 40 0d 00 00 00 00 00 76 92 cd 00 00 00 00 00 00 39 92 00 00 44 cd 00 00 6f 6f 04 00 51 d3 05 00 a7 80 0a 00 fb 7e 15 00 04 97 0a 00 69 85 24 00 4d 2f 01 00 74 16 0f 00 00 00 00 00 30 fe 14 00 c0 72 04	.....;.~`.).....Zb ....}..... .....T.....q.. .....q.....~..... .....@.....n..B.... .....@.....v.....9...D. ..oo..Q.....~.....i.$.M/.. t.....0....r.	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	unknown	13150	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 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 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	....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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE342.tmp.dmp	unknown	120	03 00 00 00 c4 00 00 00 08 07 00 00 04 00 00 00 7c 18 00 00 d8 07 00 00 0e 00 00 00 24 00 00 00 54 20 00 00 05 00 00 00 74 01 00 00 02 38 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 d8 23 00 00 e4 b5 00 00 15 00 00 00 ec 01 00 00 78 20 00 00 16 00 00 00 98 00 00 00 64 22 00 00	.....|.....$...T.....t....8.....`...8.....T.....#.....x .....d"..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 38 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.8.6.0.<./.P.i.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 31 00 39 00 37 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.>.5.3.1.9.7.<./.U.p.t.i.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 36 00 35 00 38 00 35 00 39 00 33 00 32 00 38 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.>.1.6.5.8.5.9.3.2.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 36 00 35 00 35 00 38 00 34 00 38 00 39 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.6.5.5.8.4.8.9.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 33 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.>.3.7.1.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 39 00 30 00 32 00 34 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.>.1.2.9.0.2.4.0.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 36 00 39 00 37 00 36 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.2.6.9.7.6.0.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 34 00 32 00 30 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.>.2.4.2.0.4.0.<./.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 33 00 39 00 39 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.3.9.9.6.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 33 00 36 00 37 00 32 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.>.3.6.7.2.0.<./.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 33 00 36 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.6.4.4.8.<./.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 36 00 35 00 39 00 34 00 35 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.5.9.4.5.6.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 31 00 35 00 35 00 37 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.7.1.5.5.7.1.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 36 00 35 00 39 00 34 00 35 00 36 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.6.5.9.4.5.6.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.9.8.0.<./.P.i.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 37 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.>.5.3.7.9.1.<./.U.p.t.i.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 36 00 31 00 32 00 31 00 34 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.6.1.2.1.4.7.2.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 35 00 37 00 31 00 38 00 34 00 32 00 35 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.7.1.8.4.2.5.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 38 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.9.8.9.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 36 00 39 00 36 00 33 00 32 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.>.6.9.6.3.2.0.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 36 00 38 00 35 00 36 00 37 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.8.5.6.7.0.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 31 00 35 00 34 00 34 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.>.1.1.5.4.4.8.<./.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 30 00 37 00 35 00 37 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.>.1.0.7.5.7.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.1.0.1.6.8.<./.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.6.2.4.<./.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 31 00 39 00 38 00 32 00 34 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.>.1.9.8.2.4.6.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 31 00 39 00 39 00 30 00 36 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.>.1.9.9.0.6.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 31 00 39 00 38 00 32 00 34 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.>.1.9.8.2.4.6.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.B.E.X.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	9	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 73 00 77 00 71 00 75 00 73 00 73 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.>.s.w.q.u.s.s.,. .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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 73 00 77 00 71 00 75 00 73 00 73 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.>.s.w.q.u.s.s.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 36 00 32 00 30 00 38 00 31 00 34 00 35 00 39 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.2.0.8.1.4.5.9.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 42 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.B.<./.F.l.a.g.s.>.	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 35 00 2d 00 30 00 35 00 54 00 30 00 34 00 3a 00 34 00 34 00 3a 00 35 00 39 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.-.0.5.-.0.5.T.0.4.:.4.4.:.5.9.Z.".>.	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	266	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 34 00 38 00 36 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 35 00 31 00 34 00 39 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 35 00 31 00 34 00 39 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.4.2.". .P.I.D.=.".4.8.6.0.". .U.p.t.i.m.e.M.S.=.".4.5.1.4. 9.". .T.i.m.e.S.i.n.c.e.C.r.e. a.t.i.o.n.M.S.=.".4.5.1.4.9.". .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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 35 00 62 00 66 00 32 00 34 00 66 00 39 00 2d 00 35 00 35 00 62 00 30 00 2d 00 34 00 63 00 38 00 31 00 2d 00 38 00 63 00 34 00 31 00 2d 00 66 00 35 00 30 00 32 00 37 00 38 00 30 00 33 00 34 00 65 00 31 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.3.5.b.f.2.4.f.9.-.5.5.b.0.-.4.c.8.1.-.8.c.4.1.-.f.5.0.2.7.8.0.3.4.e.1.2.<./.G.u.i.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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 35 00 2d 00 30 00 35 00 54 00 30 00 34 00 3a 00 34 00 34 00 3a 00 35 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.0.5.T.0.4.:.4.4.:.5.9.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF66D.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	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF833.tmp.xml	unknown	4766	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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_868973c6c77b45498eb43d99595a7fe2138962a_82810a17_1682f88f\Report.wer	unknown	2	ff fe	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_868973c6c77b45498eb43d99595a7fe2138962a_82810a17_1682f88f\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	184	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_868973c6c77b45498eb43d99595a7fe2138962a_82810a17_1682f88f\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 33 00 39 00 33 00 31 00 30 00 37 00 33 00 32 00	M.e.t.a.d.a.t.a.H.a.s.h.=.3.9.3.1.0.7.3.2.	success or wait	1	702A497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702C36BF	unknown
\REGISTRY\A\{bc396e13-e20a-1ede-2d56-07478b4885f1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702A43D1	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	74 03 00 C0 01 00 00 00 00 00 00 00 79 8E EC 77 01 00 00 00 90 58 F0 77 00 00 00 00 0A 00 00 00 CC F7 63 02 00 00 64 02 00 00 00 00 0A 00 00 00 88 F7 63 02 00 00 00 00 24 F8 63 02 F0 17 E6 77 B0 3F F7 BC FE FF FF FF F0 F7 63 02 D1 86 E4 77	05 00 00 C0 00 00 00 00 00 00 00 00 00 00 10 02 00 00 00 08 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	702C1FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: 5168 Parent PID: 5980

General

Start time:	21:44:55
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',DllCanUnloadNow
Imagebase:	0x1c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000010.00000002.489951685.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4788 Parent PID: 5980

General

Start time:	21:44:55
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',DllGetClassObject
Imagebase:	0x1c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000011.00000002.489294314.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5188 Parent PID: 5980

General

Start time:	21:44:56
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',WdiAddFileToInstance
Imagebase:	0x1c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000012.00000002.486848351.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5204 Parent PID: 5980

General

Start time:	21:44:57
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',WdiAddParameter
Imagebase:	0x1c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000013.00000002.488379155.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5220 Parent PID: 5980

General

Start time:	21:44:57
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',WdiCancel
Imagebase:	0x1c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000014.00000002.480983725.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 4240 Parent PID: 5168

General

Start time:	21:46:10
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5168 -s 752
Imagebase:	0xa80000
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	702D1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1982.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1982.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_10f0240f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_10f0240f\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1982.tmp	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	success or wait	1	702C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	success or wait	1	702C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1982.tmp.xml	success or wait	1	702C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EA1.tmp.csv	success or wait	1	702C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB2.tmp.txt	success or wait	1	702C4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 15 23 92 60 a4 05 12 00 00 00 00 00	MDMP..... .....#.`.....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.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 80 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 30 14 00 00 c7 22 92 60 08 00 00 00 11 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 3d 00 00 00 00 00 00 00 02 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 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....... .... ..GenuineIntelW...........T... ....0....".`.................. ....0..=............... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e................... ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.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 a8 02 02 00 00 00 c0 58 f0 77 90 58 f0 77 01 00 00 00 d4 f9 58 02 44 fa 58 02 79 8e ec 77 23 00 00 00 46 02 00 00 b0 f9 58 02 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 aa aa aa	....+...S...+. ..+............X.w.X.w......X. D.X.y..w#...F.....X.+.........	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	unknown	168	d0 06 00 00 00 00 00 00 74 03 00 c0 01 00 00 00 00 00 00 00 00 00 00 79 8e ec 77 00 00 00 00 01 00 00 00 00 00 00 00 90 58 f0 77 00 00 00 00 fc 7f f7 ff ff ff ff 0a 00 00 00 00 00 00 1c fa 58 02 00 00 00 00 00 00 59 02 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 d8 f9 58 02 00 00 00 00 00 00 00 00 00 00 00 74 fa 58 02 00 00 00 00 f0 17 e6 77 00 00 00 00 ec 50 7b be ff ff ff ff fe ff ff ff ff ff ff 40 fa 58 02 00 00 00 00 d1 86 e4 77 00 00 00 00 cc 02 00 00 8a 26 00 00	........t.....y..w.. ....X.w..... ......X.......Y..... ....X.....t.X..... ...w.....P{.....@.X... .....w.....&..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	unknown	20	0f 00 00 00 f9 8d ec 77 00 00 00 00 00 01 00 00 ae 32 00 00	.......w.....2..	success or wait	15	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	unknown	256	eb 42 fa ff 89 55 84 89 4d 8c 64 a1 30 00 00 00 8a 40 02 84 c0 75 10 a0 d4 02 fe 7f 24 03 3c 03 0f 94 c0 84 c0 74 2d 51 68 c8 da e0 77 6a 00 6a 65 e8 f1 c8 fd ff 83 c4 10 83 7d 08 00 74 15 83 65 fc 00 cc eb 07 33 c0 40 c3 8b 65 e8 c7 45 fc fe ff ff 33 c9 41 89 4d fc 8b 45 8c 89 45 90 89 4d 94 83 65 98 00 c7 45 9c f0 de e6 77 89 4d a0 8b 45 84 89 45 a4 8d 45 90 50 e8 77 50 fa ff eb 36 8b 4d ec 8b 01 8b 00 89 85 7c ff ff ff 89 4d 88 89 45 80 6a 00 8b 45 88 ff 70 04 8b 45 88 ff 30 e8 90 7d fd ff ff 75 80 6a ff e8 16 09 f9 ff 33 c0 40 c3 8b 65 e8 c7 45 fc fe ff ff ff e8 73 42 fa ff c2 04 00 8b ff 55 8b ec 51 0f b7 01 66 85 c0 74 2d 8b 51 04 d1 e8 8d 4a fe 8d 0c 41 eb 1c 0f b7 01 83 f8 5c 74 18 83 f8 40 73 0c 0f b6 80 f0 da e0 77 83 e0 08 75 0d 83 e9 02 3b	.B...U..M.d.0....@...u.....$. <.....t-Qh...wj.je.....}. .t..e.....3.@..e..E.....3.A.M. .E..E..M..e...E....w.M..E..E. .E.P.wP...6.M.....|....M..E.j ..E..p..E..0..}...u.j.....3.@ ..e..E.....sB.....U..Q...f..t- .Q....J...A.....\t...@s.. .....w...u....;	success or wait	14	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	unknown	5148	bc 9a e5 77 f2 1d ea 77 aa aa aa aa 18 ec 58 02 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 5c f1 58 02 00 00 00 00 ec 02 00 00 00 00 00 00 00 00 00 00 ec 02 00 00 14 03 00 00 b0 ec 58 02 aa aa aa aa b0 ec 58 02 12 12 ea 77 14 03 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 50 ec 58 02 aa aa aa aa 00 00 00 00 aa aa aa aa 90 ee 58 02 40 ee 58 02 14 03 00 00 00 00 9b 02 04 00 00 00 f0 02 00 00 f8 02 00 00 f4 02 00 00 ec 02 00 00 00 00 00 00 ec 02 00 00 f0 02 00 00 f4 02 00 00 f8 02 00 00 aa aa aa aa 38 ec 58 02 aa aa aa aa 54 ed 58 02 f0 17 e6 77 aa aa aa aa 00 00 00 00 cc ec 58 02 91 0c ea 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 fa 58 02 a0 8e ec 77 40 ee 58 02 90 ee 58 02 00 00 00 00 e2 da e5	...w...w......X.............. ..\.X......................... ..X.......X....w............. .............P.X............ ..X.@.X...................... .... 8.X.....T.X....w..........X... .w....................D.X....w @.X...X........	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.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 00 00 00 00 00 00 00 00 00 90 58 f0 77 aa aa aa aa 00 00 00 00 28 ec 58 02 bc 9a e5 77 23 00 00 00 06 02 00 00 e8 eb 58 02 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	?............................ ....+...S...+. ..+................X.w........ (.X....w#.........X.+.........	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	unknown	48	94 10 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 50 60 02 00 00 00 00 34 f9 50 04 00 00 00 00 cc 06 00 00 4a 68 00 00 cc 02 00 00 ee 2e 00 00	....P`.....4.P... ......Jh..........	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	unknown	4	35 00 00 00	5...	success or wait	53	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.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	53	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	unknown	752	00 00 48 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 70 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 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 e0 ff 01 00 00 00 00 00 80 de 02 00 00 00 00 bc 56 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 ea 8d 03 00 00 00 00 00 7b 8f 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 a0 15 00 00 00 00 00 18 5f 0a 00 00 00 00 00 40 ff 1f 00 00 00 00 00 04 97 0a 00 00 00 00	..Ht.....0...U..s@..p&..... .....B.....B?..... .....#..... ..@A.....Zb..... .... .V.....{. .....(....._..... @.....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	unknown	10666	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	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 60 16 00 00 9c 07 00 00 05 00 00 00 f4 00 00 00 ba 31 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 e8 1d 00 00 d8 99 00 00 15 00 00 00 ec 01 00 00 fc 1d 00 00 16 00 00 00 98 00 00 00 e8 1f 00 00	....1.....T.....8..... ....T.....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 31 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.1.6.8.<./.P.i.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 38 00 33 00 30 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.>.7.8.3.0.5.<./.U.p.t.i.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 32 00 38 00 38 00 33 00 39 00 36 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.8.3.9.6.8.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 32 00 38 00 38 00 33 00 31 00 34 00 38 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.8.3.1.4.8.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 35 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.>.2.7.5.5.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 33 00 38 00 33 00 39 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.3.8.3.9.3.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 33 00 38 00 33 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.>.9.3.8.3.9.3.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 38 00 36 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 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.>.1.8.6.8.8.0.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 36 00 36 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.6.6.8.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 33 00 31 00 36 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.>.3.1.6.8.0.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 33 00 31 00 34 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.>.3.1.4.0.8.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 35 00 39 00 38 00 34 00 32 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.9.8.4.2.5.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 35 00 39 00 39 00 32 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.9.9.2.4.4.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 35 00 39 00 38 00 34 00 32 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.9.8.4.2.5.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.9.8.0.<./.P.i.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	46	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 37 00 37 00 36 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.>.1.2.7.7.6.0.<./.U.p.t.i.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 36 00 31 00 32 00 31 00 34 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.6.1.2.1.4.7.2.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 35 00 34 00 35 00 36 00 32 00 38 00 31 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.4.5.6.2.8.1.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 39 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.9.9.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 36 00 39 00 36 00 33 00 32 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.>.6.9.6.3.2.0.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 36 00 38 00 30 00 37 00 35 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.8.0.7.5.5.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 31 00 35 00 34 00 34 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.>.1.1.5.4.4.8.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 30 00 37 00 35 00 37 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.>.1.0.7.5.7.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.1.0.1.6.8.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 38 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.>.9.0.8.0.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 31 00 38 00 34 00 33 00 32 00 30 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.>.1.8.4.3.2.0.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 31 00 39 00 39 00 30 00 36 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.>.1.9.9.0.6.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 31 00 38 00 34 00 33 00 32 00 30 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.>.1.8.4.3.2.0.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 73 00 77 00 71 00 75 00 73 00 73 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.>.s.w.q.u.s.s.,. .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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 73 00 77 00 71 00 75 00 73 00 73 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.>.s.w.q.u.s.s.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 36 00 32 00 30 00 38 00 31 00 34 00 35 00 39 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.2.0.8.1.4.5.9.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 35 00 2d 00 30 00 35 00 54 00 30 00 34 00 3a 00 34 00 36 00 3a 00 31 00 33 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.-.0.5.-.0.5.T.0.4.:.4.6.:.1.3.Z.".>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	266	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 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 31 00 36 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 37 00 31 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 37 00 31 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.5.7.". .P.I.D.=.".5.1.6.8.". .U.p.t.i.m.e.M.S.=.".7.1.5.7.7.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".7.1.5.7.7.". .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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 62 00 36 00 30 00 35 00 63 00 31 00 62 00 2d 00 33 00 39 00 61 00 37 00 2d 00 34 00 37 00 64 00 38 00 2d 00 61 00 30 00 39 00 39 00 2d 00 66 00 62 00 31 00 64 00 39 00 32 00 34 00 35 00 36 00 61 00 38 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.3.b.6.0.5.c.1.b.-.3.9.a.7.-.4.7.d.8.-.a.0.9.9.-.f.b.1.d.9.2.4.5.6.a.8.7.<./.G.u.i.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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 35 00 2d 00 30 00 35 00 54 00 30 00 34 00 3a 00 34 00 36 00 3a 00 31 00 33 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.-.0.5.-.0.5.T.0.4.:.4.6.:.1.3.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER181A.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	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1982.tmp.xml	unknown	4679	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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_10f0240f\Report.wer	unknown	2	ff fe	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_10f0240f\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	184	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1d91dafffd792f9b512ff42d10d3dd5f24a3f5de_82810a17_10f0240f\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 35 00 30 00 36 00 35 00 37 00 30 00 30 00 33 00 36 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.5.0.6.5.7.0.0.3.6.	success or wait	1	702C497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{708037f5-36bd-4c92-56e3-9fa7b30c1148}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702E36BF	unknown
\REGISTRY\A\{708037f5-36bd-4c92-56e3-9fa7b30c1148}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702E36BF	unknown
\REGISTRY\A\{708037f5-36bd-4c92-56e3-9fa7b30c1148}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702C43D1	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 00 00 00 10 02 00 00 00 08 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	74 03 00 C0 01 00 00 00 00 00 00 00 79 8E EC 77 01 00 00 00 90 58 F0 77 FC 7F F7 FF 0A 00 00 00 1C FA 58 02 00 00 59 02 00 00 00 00 0A 00 00 00 D8 F9 58 02 00 00 00 00 74 FA 58 02 F0 17 E6 77 EC 50 7B BE FE FF FF FF 40 FA 58 02 D1 86 E4 77	success or wait	1	702E1FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 1760 Parent PID: 5188

General

Start time:	21:46:10
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5188 -s 756
Imagebase:	0xa80000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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	702D1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6C.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_7dd67966396113c995f4a9c30eeff967a1ce3cd_82810a17_06802046	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_7dd67966396113c995f4a9c30eeff967a1ce3cd_82810a17_06802046\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	702C497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6C.tmp	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp.dmp	success or wait	1	702C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	success or wait	1	702C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6C.tmp.xml	success or wait	1	702C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6F9D.tmp.csv	success or wait	1	702C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FBE.tmp.txt	success or wait	1	702C4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 15 23 92 60 a4 05 12 00 00 00 00 00	MDMP..... .....#.`.....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.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 80 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 44 14 00 00 c8 22 92 60 07 00 00 00 12 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 3d 00 00 00 00 00 00 00 02 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 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..... .... ..GenuineIntelW.....T... ....D....".`..... .....0..=..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.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 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 14 7e 00 10 90 bc 95 02 ff ff ff ff 14 7e 00 10 c3 0f 00 02 04 fe 67 02 14 7e 00 10 23 00 00 00 07 02 01 00 80 fd 67 02 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...+. ..+........~..........~...... ..g..~..#.........g.+.........	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp.dmp	unknown	168	44 00 00 00 00 00 00 00 94 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 14 7e 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 8a 26 00 00	D.......................~.... ....&..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp.dmp	unknown	20	0e 00 00 00 88 05 96 02 00 00 00 00 04 00 00 00 9e 32 00 00	................2..	success or wait	14	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp.dmp	unknown	4	d8 f9 22 04	..".	success or wait	13	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp.dmp	unknown	1780	bc b1 e5 77 d6 c9 e3 77 64 02 00 00 aa aa aa aa 10 00 00 00 a0 f9 22 04 6c fa 22 04 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 d0 54 02 00 d0 54 02 00 00 00 00 64 02 00 00 aa aa aa aa 64 02 00 00 aa aa aa aa 00 d0 54 02 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 aa aa aa aa 00 00 00 00 00 00 00 00 00 aa aa aa aa 88 05 96 02 00 00 00 00 00 00 00 00 e0 07 96 02 00 10 54 02 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 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 38 f9 37 04 54 12 54 02 40 f9 37 04 78 06 96 02 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	...w...wd............".I."... ..@..w@..w......T...T.....d... ....d.........T.............. ....T................ ....8.7.T. T.@.7.x......................	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.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 14 7e 00 10 00 00 00 00 18 ef 67 02 bc 9a e5 77 23 00 00 00 06 02 00 00 88 ed 67 02 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...+. ..+....................~...... ..g....w#.........g.+.........	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp.dmp	unknown	48	00 13 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 55 02 00 00 00 00 6c f8 37 04 00 00 00 00 94 07 00 00 2a 45 00 00 cc 02 00 00 ee 2e 00 00	....U.....l.7... ......*E..........	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp.dmp	unknown	4	35 00 00 00	5...	success or wait	53	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.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	53	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp.dmp	unknown	752	00 00 48 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 70 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 80 00 02 00 00 00 00 00 80 de 02 00 00 00 00 c9 56 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 d2 8d 03 00 00 00 00 00 7b 8f 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 31 a0 15 00 00 00 00 00 0f 5f 0a 00 00 00 00 00 40 ff 1f 00 00 00 00 00 04 97 0a 00 00 00 00	..Ht.....0...U..s@..p&..... .....B.....B?..... .....#..... ..@A.....Zb..... .... .V.....{. .....1....._..... @.....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp.dmp	unknown	10742	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	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11CF.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 60 16 00 00 9c 07 00 00 05 00 00 00 e4 00 00 00 ba 31 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 10 1e 00 00 30 97 00 00 15 00 00 00 ec 01 00 00 fc 1d 00 00 16 00 00 00 98 00 00 00 e8 1f 00 00	..............`..... ...1.....T.....8..... ....T.....0.....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 31 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.1.8.8.<./.P.i.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 37 00 37 00 30 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.>.7.7.7.0.5.<./.U.p.t.i.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 32 00 38 00 38 00 33 00 39 00 36 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.8.3.9.6.8.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 32 00 38 00 38 00 33 00 31 00 34 00 38 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.8.3.1.4.8.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.6.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 34 00 30 00 34 00 34 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.>.9.4.0.4.4.1.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 34 00 30 00 34 00 34 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.>.9.4.0.4.4.1.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 38 00 36 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 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.>.1.8.6.8.8.0.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 36 00 36 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.6.6.8.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 33 00 31 00 37 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.3.1.7.7.6.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 33 00 31 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.1.5.0.4.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 35 00 39 00 39 00 32 00 34 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.9.9.2.4.4.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 36 00 30 00 30 00 30 00 36 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.0.0.0.6.4.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 35 00 39 00 39 00 32 00 34 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.9.9.2.4.4.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.9.8.0.<./.P.i.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	46	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 38 00 30 00 38 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.>.1.2.8.0.8.8.<./.U.p.t.i.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 36 00 31 00 32 00 31 00 34 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.6.1.2.1.4.7.2.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 35 00 34 00 35 00 36 00 32 00 38 00 31 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.4.5.6.2.8.1.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 39 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.9.9.1.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 36 00 39 00 36 00 33 00 32 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.>.6.9.6.3.2.0.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 36 00 38 00 30 00 37 00 35 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.8.0.7.5.5.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 31 00 35 00 34 00 34 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.>.1.1.5.4.4.8.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 30 00 37 00 35 00 37 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.>.1.0.7.5.7.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.1.0.1.6.8.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 38 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.>.9.0.8.0.<./.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 31 00 38 00 34 00 33 00 32 00 30 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.>.1.8.4.3.2.0.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 31 00 39 00 39 00 30 00 36 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.>.1.9.9.0.6.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 31 00 38 00 34 00 33 00 32 00 30 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.>.1.8.4.3.2.0.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 73 00 77 00 71 00 75 00 73 00 73 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.>.s.w.q.u.s.s.,. .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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 73 00 77 00 71 00 75 00 73 00 73 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.>.s.w.q.u.s.s.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 36 00 32 00 30 00 38 00 31 00 34 00 35 00 39 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.2.0.8.1.4.5.9.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 35 00 2d 00 30 00 35 00 54 00 30 00 34 00 3a 00 34 00 36 00 3a 00 31 00 34 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.-.0.5.-.0.5.T.0.4.:.4.6.:.1.4.Z.".>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	266	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 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 31 00 38 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 37 00 31 00 33 00 39 00 30 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 37 00 31 00 33 00 39 00 30 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	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.5.9.". .P.I.D.=.".5.1.8.8.". .U.p.t.i.m.e.M.S.=.".7.1.3.9.0.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".7.1.3.9.0.". .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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 35 00 33 00 30 00 39 00 36 00 39 00 30 00 2d 00 38 00 64 00 61 00 31 00 2d 00 34 00 35 00 30 00 34 00 2d 00 62 00 66 00 33 00 39 00 2d 00 65 00 34 00 63 00 61 00 63 00 35 00 37 00 66 00 61 00 64 00 30 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.5.5.3.0.9.6.9.0.-.8.d.a.1.-.4.5.0.4.-.b.f.3.9.-.e.4.c.a.c.5.7.f.a.d.0.4.<./.G.u.i.d.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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 35 00 2d 00 30 00 35 00 54 00 30 00 34 00 3a 00 34 00 36 00 3a 00 31 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.0.5.T.0.4.:.4.6.:.1.4.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.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	702C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A6C.tmp.xml	unknown	4665	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 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	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_7dd67966396113c995f4a9c30eeff967a1ce3cd_82810a17_06802046\Report.wer	unknown	2	ff fe	..	success or wait	1	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_7dd67966396113c995f4a9c30eeff967a1ce3cd_82810a17_06802046\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	184	702C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_7dd67966396113c995f4a9c30eeff967a1ce3cd_82810a17_06802046\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 38 00 37 00 30 00 35 00 30 00 33 00 30 00 39 00 31 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.8.7.0.5.0.3.0.9.1.	success or wait	1	702C497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 3492 Parent PID: 4788

General

Start time:	21:46:11
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4788 -s 760
Imagebase:	0xa80000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 5172 Parent PID: 5204

General

Start time:	21:46:11
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5204 -s 756
Imagebase:	0xa80000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis