ID: 404283
Sample Name:
fc0bc077_by_Libranalysis
Cookbook: default.jbs
Time: 21:32:56
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

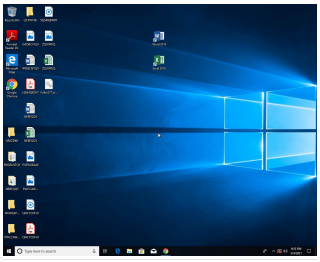
Analysis Report fc0bc077_by_Libranalysis

Overview

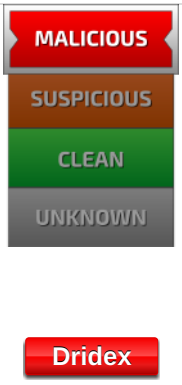
General Information

Sample Name:	fc0bc077_by_Libranalysis (renamed file extension from none to dll)
Analysis ID:	404283
MD5:	fc0bc07721ce94b..
SHA1:	2d98f05fb78cd75..
SHA256:	e707edac036a1a..
Tags:	Dridex
Infos:	

Most interesting Screenshot:



Detection

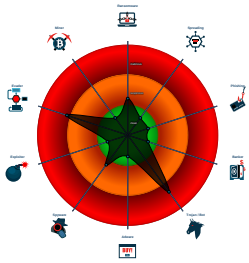


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 process in suspended mo…
- Detected potential crypto function
- IP address seen in connection with o…
- Internet Provider seen in connection…
- One or more processes crash

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5800 cmdline: loaddll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5496 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4836 cmdline: rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6728 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4836 -s 760 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5480 cmdline: rundll32.exe C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll,LoxmtYt MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7000 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5480 -s 928 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7032 cmdline: rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',DllCanUnloadNow MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 4260 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7032 -s 752 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7100 cmdline: rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',DllGetClassObject MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7136 cmdline: rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',WdiAddFileToInstance MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 776 cmdline: rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',WdiAddParameter MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6232 cmdline: rundll32.exe 'C:\Users\user\Desktop\fc0bc077_by_Libranalysis.dll',WdiCancel MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 6316 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5800 -s 580 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **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

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.494169228.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

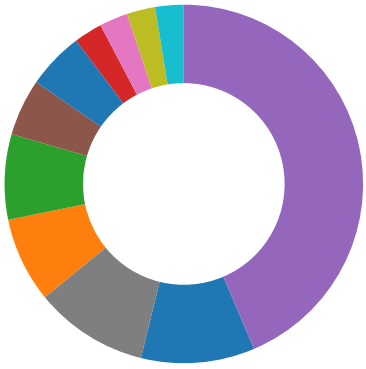
Unpacked PEs

Source	Rule	Description	Author	Strings
19.2.rundll32.exe.10000000.3.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

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

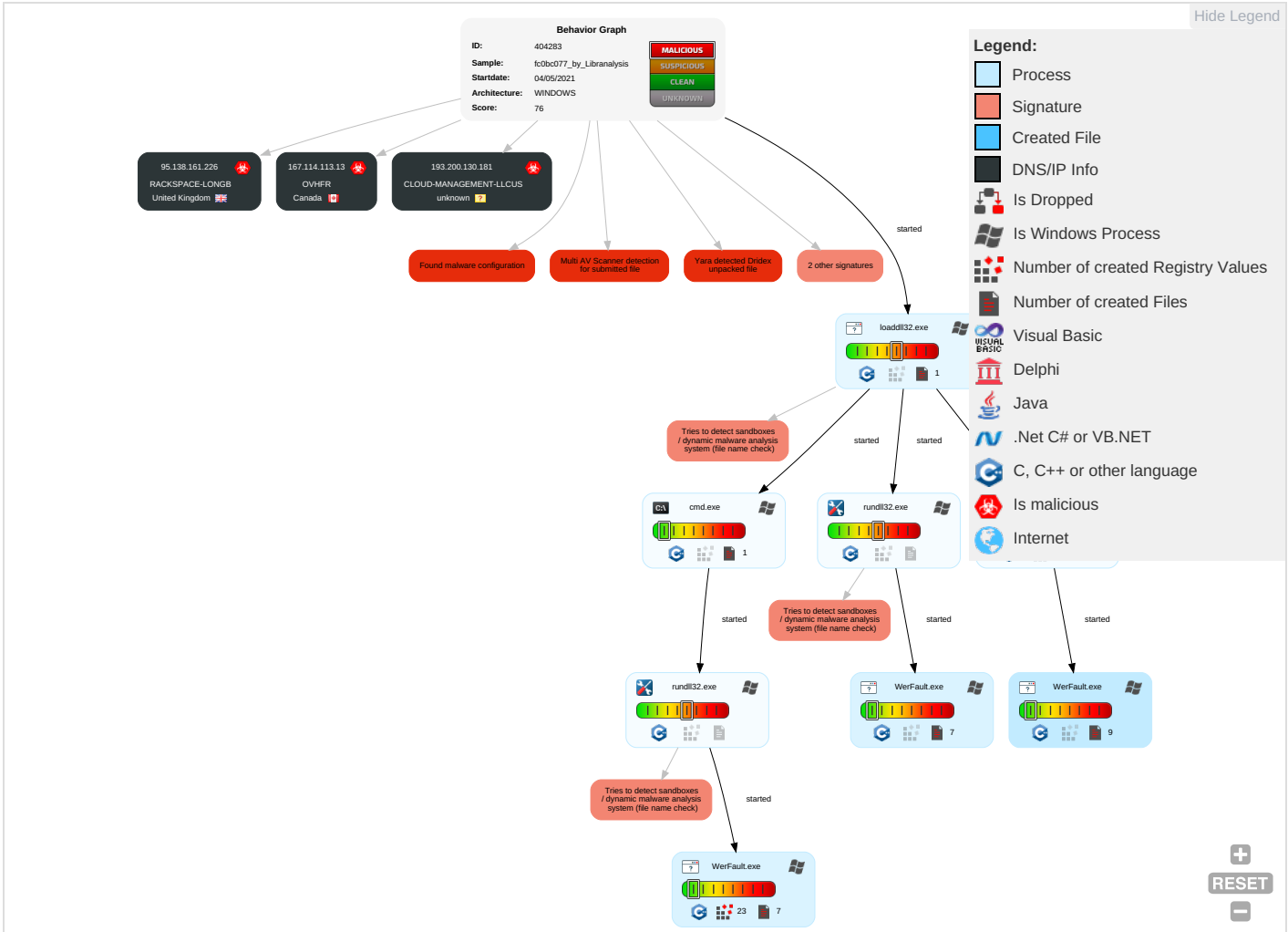
Malware Analysis System Evasion:

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	OS Credential Dumping	Security Software Discovery 1 1 1	Remote Services	Archive Collected Data 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	Data from Removable Media	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

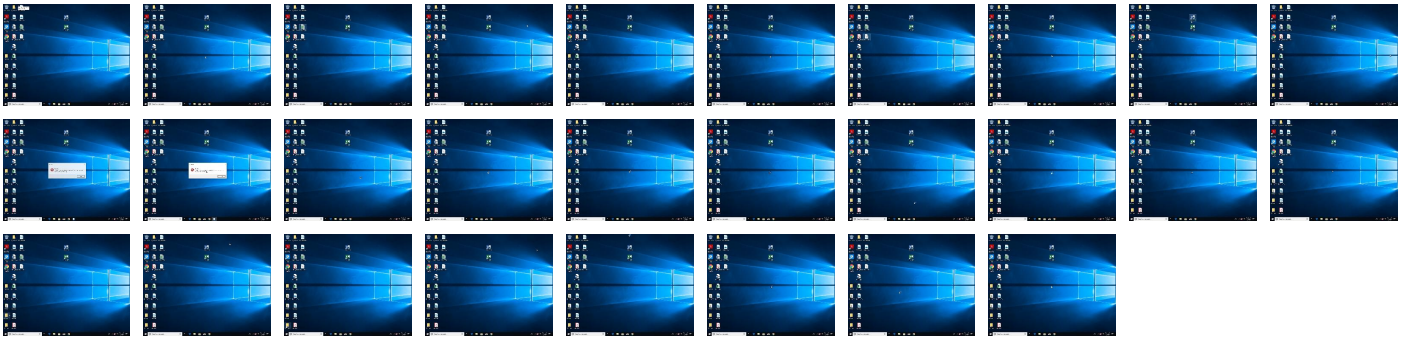
Behavior Graph



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	

Source	Detection	Scanner	Label	Link
fc0bc077_by_Libranalysis.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
19.2.rundll32.exe.590607.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.rundll32.exe.5b0000.2.unpack	100%	Avira	TR/ATRAPS.Gen2		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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404283
Start date:	04.05.2021
Start time:	21:32:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fc0bc077_by_Libranalysis (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	32
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@21/7@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 95.2% (good quality ratio 93.5%) • Quality average: 78.4% • Quality standard deviation: 25.7%
HCA Information:	• Successful, ratio: 75% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

Time	Type	Description
21:34:37	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
167.114.113.13	e1c88b94_by_Libranalysis.dll	Get hash	malicious	Browse	
	8743016c_by_Libranalysis.dll	Get hash	malicious	Browse	
	d8417415_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	64b8ed95_by_Libranalysis.dll	Get hash	malicious	Browse	
	c85a75aa_by_Libranalysis.dll	Get hash	malicious	Browse	
	c977c96e_by_Libranalysis.dll	Get hash	malicious	Browse	
	b8dd7ed8_by_Libranalysis.dll	Get hash	malicious	Browse	
	af1e75cf_by_Libranalysis.dll	Get hash	malicious	Browse	
95.138.161.226	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	
	64b8ed95_by_Libranalysis.dll	Get hash	malicious	Browse	
	c85a75aa_by_Libranalysis.dll	Get hash	malicious	Browse	
	c977c96e_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	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
	64b8ed95_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	c85a75aa_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	c977c96e_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
	b8dd7ed8_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	af1e75cf_by_Libranalysis.dll	Get hash	malicious	Browse	• 95.138.161.226
CLOUD-MANAGEMENT-LLCUS	e1c88b94_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	8743016c_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	d8417415_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	9a46403f_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	edae86a8_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	457aedfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	64b8ed95_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	8743016c_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	d8417415_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	c977c96e_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	9a46403f_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	457aedfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	edae86a8_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	b8dd7ed8_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	af1e75cf_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	64b8ed95_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	c85a75aa_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	c977c96e_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	b8dd7ed8_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
	af1e75cf_by_Libranalysis.dll	Get hash	malicious	Browse	• 193.200.130.181
OVHFR	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
	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
	64b8ed95_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	c85a75aa_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	c977c96e_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\Temp\WER58E4.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):	3.692806116875498
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiU4616Y/k6rDgmf8GHS5CpBW89bwnhsfNwm:RrlsNiT616YM6rDgmf8US8wnafv
MD5:	87D22F12DBDB2F159700C25E44D7BBE2
SHA1:	4626A03A64F12D738E5B554AA26EA61982C7F290
SHA-256:	015FA8D5B4E37F7C0F294FB4D7E1770805720833073E42EAFB831DBC0AAD67C8
SHA-512:	CFB0DDEB4D1C07B60FF923E00CAF0EDCA0F23881A08580C3B3BD9F94704B90DD9EFC08E0A6AF42F66C2120C6F333579F7C5D7A6734336805FF2A98A694A1882E
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.>.5.4.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C49.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):	4.461586416167699
Encrypted:	false
SSDEEP:	48:cvIwSD8zsQJgtWI9LTWSC8BX/8fm8M4JCdskN4fFiY+q8vjskN4yhV54SrSjd:uITfWkiSNKJ2N4jKrN40V5DWjd
MD5:	4B7B1D196E97FE65F8D7D4A351A9D63B
SHA1:	694854501C58379C4287E3C724E61970AABC78B0
SHA-256:	EFC9F086B2EB8EB455805B1DFF7DDA61266709CC295E09442294DCD547BC5281
SHA-512:	0C2087B087403D08A030A46408630F9B65BA6C33AD2FA1978BC809BCFD355E6EFA6E42649EC5B44C742D5A21D2410298D41CD6104CBB6FF2675EEAC2698AD60
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="975706" />.. <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\WER9F18.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 5 04:34:39 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	40228
Entropy (8bit):	2.4948280065301587
Encrypted:	false
SSDEEP:	192:I5OyvPAmrgBjAgXJgo/5IHP5TMfsMocwMEU7G3aLsGHrb71RMu/PfMNd9Zln:fCYQgBkgXJ9sPZJY2esGrbbH/Pa/n
MD5:	B3C703888E53812262ED07B180BFC1A5
SHA1:	3096346789F4544532DA8EC62677E3932D713B49
SHA-256:	DC23C05FC18D6CDA16C850784E0D9FB7EE7BA6448CC028F9F8068273431FE6FE
SHA-512:	892648D861ADDD1FED9B57F271323F44A725BB5F578B653AEDBC407169C4BDD0A09BC6A1E6BF04C1C81E5372B6800DA45B9491C62E2F99CBCC59D00ACCFA2E4
Malicious:	false
Preview:	MDMP..... ....._ .`.....U.....B.....P .....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\WERADCE.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp.dmp	
File Type:	Mini DuMP crash report, 15 streams, Wed May 5 04:35:07 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	49052
Entropy (8bit):	2.30173230730282
Encrypted:	false
SSDEEP:	192:UPlVjsfPTbCAbnzsgoZQKeuje5XOagyiIEpmzq9nZDxmuxS:qlVgfSSwgqHjsXngz5pp/a
MD5:	066E444520FEFBA46B30B618412DCC7F
SHA1:	B25BAC021E8B7777974C85E2DBAE9F347CACE85C
SHA-256:	2202877BF640155BB85B986561A9BD5A7C96F3529DC59B928D31EDC700226122
SHA-512:	E153981020D362338497BFBE29F5F66041F9AD064BAAAA4931952BD29528DCD60914214EB21F80347E9A91507C34DB9A3E8852A6111636D1799BB3BFB1576CEB
Malicious:	false
Preview:	MDMP..... .....{ .`.....U.....B....."....GenuineIntelW.....T.....h...+ .`.....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\WERAE7B.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):	3.701679402457719
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNik269r6YV+6OkgmfTHjSX8CprP89bSnYsfwTmm:RrlsNid6h6Y86OkgmfTHjSESnLfwb
MD5:	6674D2BA58A6826CD1EB20E890CC9ADC
SHA1:	3664890381B7FD8A5F79B2DD85777B34C66B48CE
SHA-256:	19AE4DB3B3A388FB6B085586411AD4C7D061CC8DB5B5ECB5CC0F67710ECAC1C5
SHA-512:	6FF3268B0F3855226A7D00DEF77504054CBA1E4A5D3F74C38FD6A95732E998B2AF2488129E540D5A4AA6898C7531455A5151C7AEACFA2F1DCD7335D3AA0EF47
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.>.4.8.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1D7.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):	4.511580448811392
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5JgtWI9LTWSC8BF8fm8M4JCdsnZFwpn+q8/3UwV54SrSYd:ulTfLkiSNwJVspjwV5DWYd
MD5:	A60A92E323E8DA233931E9A35B09C953
SHA1:	97C145F6566B503E5264E13633EB0F306A0883B1
SHA-256:	D9B578D4BC6DD62195E8282BDF51CA74B29D81C339E7148C4BD75FDFCCFE5C7E
SHA-512:	1EDFEB3F77B909D17E3BC830719AA0F64C8516E786FAB407B2DAB97D301DE255A86268355B6FD7B2DC1C5D71A4927078112AF434C1B488DEAA1F7B5032F47F7
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="975705" />.. <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\WERF47C.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

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
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
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	

Name	Virtual Address	Virtual Size	Is in Section
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

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5800 Parent PID: 5680

General

Start time:	21:33:46
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:	0xf90000
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: 5496 Parent PID: 5800

General

Start time:	21:33:46
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:	0x870000
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: 5480 Parent PID: 5800

General

Start time:	21:33:47
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:	0x10d0000
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: 4836 Parent PID: 5496

General

Start time:	21:33:47
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:	0x10d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 6728 Parent PID: 4836

General

Start time:	21:34:31

Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4836 -s 760
Imagebase:	0x1200000
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	6F6E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1D7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1D7.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1D7.tmp	success or wait	1	6F6D497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 5f 20 92 60 a4 05 12 00 00 00 00 00	MDMP..... ....._ .`.....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.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 50 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 e4 12 00 00 2b 20 92 60 06 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 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......P .... ..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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.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 dd 00 02 00 00 00 c0 58 3b 77 90 58 3b 77 01 00 00 00 cc fa a7 00 3c fb a7 00 79 8e 37 77 23 00 00 00 46 02 00 00 a8 fa a7 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+............X;w.X;w........ <...y.7w#...F.......+.........	success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp.dmp	unknown	168	c8 0c 00 00 00 00 00 00 74 03 00 c0 01 00 00 00 00 00 00 00 00 00 00 00 79 8e 37 77 00 00 00 00 01 00 00 00 00 00 00 90 58 3b 77 00 00 00 00 0a 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 14 fb a7 00 00 00 00 00 00 a8 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 d0 fa a7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6c fb a7 00 00 00 00 00 f0 17 31 77 00 00 00 00 97 81 15 39 00 00 00 00 fe ff ff ff ff ff ff ff 38 fb a7 00 00 00 00 00 d1 86 2f 77 00 00 00 00 cc 02 00 00 5a 26 00 00	.....t.....y.7w.. .....X;w..... ....I..... ..1w.....9.....8..... ..../w.....Z&..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp.dmp	unknown	20	0c 00 00 00 3c 9a 30 77 00 00 00 00 00 00 01 00 00 82 2f 00 00	....<.0w...../..	success or wait	12	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp.dmp	unknown	256	c2 08 00 90 b8 54 00 00 00 ba e0 dc 31 77 ff d2 c2 18 00 90 b8 55 00 00 00 ba e0 dc 31 77 ff d2 c2 2c 00 90 b8 56 00 00 00 ba e0 dc 31 77 ff d2 c2 14 00 90 b8 57 00 00 00 ba e0 dc 31 77 ff d2 c2 18 00 90 b8 58 00 00 00 ba e0 dc 31 77 ff d2 c2 0c 00 90 b8 59 00 00 00 ba e0 dc 31 77 ff d2 c2 40 00 90 b8 5a 00 18 00 ba e0 dc 31 77 ff d2 c2 04 00 90 b8 5b 00 1d 00 ba e0 dc 31 77 ff d2 c2 14 00 90 b8 5c 00 00 00 ba e0 dc 31 77 ff d2 c2 10 00 90 b8 5d 00 00 00 ba e0 dc 31 77 ff d2 c2 08 00 90 b8 5e 00 00 00 ba e0 dc 31 77 ff d2 c2 10 00 90 b8 5f 00 00 00 ba e0 dc 31 77 ff d2 c2 14 00 90 b8 60 00 00 00 ba e0 dc 31 77 ff d2 c2 18 00 90 b8 61 00 07 00 ba e0 dc 31 77 ff d2 c2 08 00 90 b8 62 00 00 00 ba e0 dc 31 77 ff d2 c2 1c 00 90 b8 63 00 00 00 ba e0 dc 31 77 ff	.....T.....1w.....U.....1w ...,...V.....1w.....W..... 1w.....X.....1w.....Y.... ..1w...@...Z.....1w.....[.. ....1w.....\.....1w.....] .....1w.....^.....1w..... ._.....1w.....`.....1w.... ...a.....1w.....b.....1w.. .....c.....1w.	success or wait	11	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp.dmp	unknown	2312	bc b1 30 77 d6 c9 2e 77 70 02 00 00 aa aa aa aa 10 00 00 00 8c f7 00 01 58 f8 00 01 aa aa aa aa 40 c7 2e 77 40 c7 2e 77 a8 07 de 00 00 00 8a 00 00 00 8a 00 00 00 00 00 70 02 00 00 aa aa aa aa 70 02 00 00 aa aa aa aa 00 00 8a 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 60 d7 de 00 00 00 00 00 00 00 00 48 09 de 00 00 40 89 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a8 07 de 00 00 00 00 00 aa aa aa aa aa aa aa aa 54 42 89 00 54 42 89 00 e0 07 de 00 e0 07 de 00 00 00 00 00 aa aa aa aa a8 07 de 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..0w...wp..............X..... ..@..w@..w................p... ....p......................... ....`..... ......H....@.................. ....TB..TB	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp.dmp	unknown	4	02 00 00 00	....	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.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 3b 77 aa aa aa aa 00 00 00 00 20 ed a7 00 bc 9a 30 77 23 00 00 00 12 02 00 00 e0 ec a7 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+................X;w........ .....0w#...........+.........	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp.dmp	unknown	48	e8 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 00 8a 00 00 00 00 00 f8 f6 00 01 00 00 00 00 08 09 00 00 4e 6a 00 00 cc 02 00 00 f2 2b 00 00	....Nj.......+..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp.dmp	unknown	4	35 00 00 00	5...	success or wait	53	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp.dmp	unknown	752	00 00 93 73 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 40 26 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 30 4b 02 00 00 00 00 00 60 d7 02 00 00 00 00 23 4b 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 17 6d 03 00 00 00 00 00 2c 6d 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 49 15 00 00 00 00 00 1d b6 0a 00 00 00 00 00 40 ff 1f 00 00 00 00 00 20 dd 0a 00 00 00 00	...s.....0...U..s@..@&..... .....B.....B?..... .....#..... ..@A.....Zb..... ....0K.....`..... #K.....m.....,m .....#I.....@.....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp.dmp	unknown	10774	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 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 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	....E.v.e.n.t..... .....F.i.l.e.....F.i.l.e... (...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	success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F18.tmp.dmp	unknown	108	03 00 00 00 64 00 00 00 fc 06 00 00 04 00 00 00 60 16 00 00 6c 07 00 00 05 00 00 00 c4 00 00 00 be 2e 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 34 7f 00 00 15 00 00 00 ec 01 00 00 cc 1d 00 00 16 00 00 00 98 00 00 00 b8 1f 00 00	....d.....`...l..... .....T.....8..... ....T.....8...4.....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 38 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.8.3.6.<./.P.i.d.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 32 00 31 00 37 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.>.5.2.1.7.3.<./.U.p.t.i.m.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 33 00 31 00 35 00 33 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.3.1.5.3.9.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 33 00 30 00 37 00 32 00 30 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.3.0.7.2.0.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 37 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.>.2.7.5.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 36 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.6.6.5.6.<./.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.6.4.5.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 33 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.3.1.3.4.4.<./.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.1.0.7.2.<./.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 38 00 39 00 30 00 30 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.>.5.8.9.0.0.4.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 38 00 39 00 38 00 32 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.>.5.8.9.8.2.4.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 38 00 39 00 30 00 30 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.>.5.8.9.0.0.4.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 34 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.4.9.6.<./.P.i.d.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 32 00 35 00 39 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.2.5.9.9.<./.U.p.t.i.m.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.2.5.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 33 00 35 00 35 00 35 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.>.3.7.3.5.5.5.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 39 00 38 00 36 00 38 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.6.9.8.6.8.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 35 00 30 00 32 00 36 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.>.2.5.0.2.6.5.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 36 00 31 00 32 00 36 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.1.2.6.7.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 35 00 30 00 32 00 36 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.>.2.5.0.2.6.5.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 63 00 73 00 68 00 69 00 68 00 79 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.>.c.s.h.i.h.y.,. .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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 63 00 73 00 68 00 69 00 68 00 79 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.>.c.s.h.i.h.y.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 37 00 36 00 31 00 37 00 36 00 37 00 34 00 35 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.>.1.5.7.6.1.7.6.7.4.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 33 00 34 00 3a 00 33 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.:.3.4.:.3.9.Z.".>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 33 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 38 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 31 00 37 00 39 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 31 00 37 00 39 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.3.9.". .P.I.D.=.".4.8.3.6.". .U.p.t.i.m.e.M.S.=.".4.1.7.9.6.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".4.1.7.9.6.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 31 00 37 00 61 00 38 00 66 00 32 00 65 00 2d 00 39 00 38 00 31 00 36 00 2d 00 34 00 32 00 63 00 36 00 2d 00 39 00 61 00 63 00 38 00 2d 00 35 00 33 00 64 00 65 00 64 00 36 00 65 00 35 00 65 00 37 00 61 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.8.1.7.a.8.f.2.e.-.9.8.1.6.-.4.2.c.6.-.9.a.c.8.-.5.3.d.e.d.6.e.5.e.7.a.9.<./.G.u.i.d.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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 33 00 34 00 3a 00 33 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.:.3.4.:.3.9.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7B.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	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1D7.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	6F6D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6F6F36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6F6F1FB2	RegCreateKeyExW
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6D43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LongPathHash	unicode	rundll32.exe\ab97b57a	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6F6F36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6F6F36BF	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 37 77 01 00 00 00 90 58 3B 77 0A 00 00 00 0A 00 00 00 14 FB A7 00 00 00 A8 00 00 00 00 00 0A 00 00 00 D0 FA A7 00 00 00 00 00 6C FB A7 00 F0 17 31 77 97 81 15 39 FE FF FF FF 38 FB A7 00 D1 86 2F 77	success or wait	1	6F6F1FE8	RegSetValueExW

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

Analysis Process: WerFault.exe PID: 7000 Parent PID: 5480

General

Start time:	21:34:34
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5480 -s 928
Imagebase:	0x1200000
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	6F6E1717	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C49.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C49.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C49.tmp	success or wait	1	6F6D497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 7b 20 92 60 a4 05 12 00 00 00 00 00	MDMP........ ....{ .`........	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.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 cc 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 68 15 00 00 2b 20 92 60 07 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... ....h...+ .`................. ....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	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.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 10 00 fb 4f 00 00 00 00 00 ff ff ff ff 00 00 00 10 00 00 00 00 0c fb 4f 00 00 00 00 10 23 00 00 00 46 02 01 00 f0 fa 4f 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.........O................ ..O.....#...F.....O.+.........	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp.dmp	unknown	168	6c 15 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 00 00 00 cc 02 00 00 d6 29 00 00	l............................ ....)..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp.dmp	unknown	20	10 00 00 00 e0 f8 98 00 00 00 00 00 20 07 00 00 0a 36 00 00	....6..	success or wait	16	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp.dmp	unknown	1824	bc b1 30 77 d6 c9 2e 77 5c 02 00 00 aa aa aa aa 10 00 00 00 74 f9 98 00 40 fa 98 00 aa aa aa aa 40 c7 2e 77 40 c7 2e 77 aa aa aa aa 00 a0 71 00 00 a0 71 00 00 00 00 00 5c 02 00 00 aa aa aa aa 5c 02 00 00 aa aa aa aa 00 a0 71 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 70 29 9f 00 00 00 00 00 00 00 00 00 48 08 9e 00 00 10 71 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 8c fb 0b 01 54 12 71 00 94 fb 0b 01 e0 06 9e 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	..0w...w\...........t...@..... ..@..w@..w......q...q.....\... ....\.........q............... ....p).... ......H.....q................. ....T. q.............................	success or wait	15	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp.dmp	unknown	4096	6c fc 0b 01 00 00 0c 01 00 40 0b 01 00 00 00 00 00 1e 00 00 00 00 00 00 00 d0 71 00 00 00 00 00 68 15 00 00 bc 19 00 00 00 00 00 00 00 00 00 00 00 10 71 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 29 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 00 00 00 00 00	l........@................q... ..h................q......... ....p)w.............	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.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 58 ed 4f 00 bc 9a 30 77 23 00 00 00 06 02 00 00 18 ed 4f 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+.......................... X.O...0w#.........O.+.........	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp.dmp	unknown	48	bc 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 d0 71 00 00 00 00 00 00 c0 fa 0b 01 00 00 00 00 00 40 05 00 00 2a 3d 00 00 cc 02 00 00 3a 32 00 00	....q........... ..@...*=......:2..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp.dmp	unknown	4	3a 00 00 00	:...	success or wait	58	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp.dmp	unknown	120	00 00 0e 6f 00 00 00 00 00 60 0d 00 20 d1 0d 00 aa 0c c7 bd 7a 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 00 25 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 0c 00 00 00 18 00 00 00 01 00 00 00	...o.....`.. ....z)........ ....B.......B?........... ....%............ ..@A.........................	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.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	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp.dmp	unknown	668	00 00 00 10 00 00 00 00 00 00 10 02 00 00 00 00 00 00 3b cc 7e 60 98 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 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 d0 25 02 00 00 00 00 00 60 d7 02 00 00 00 00 11 4c 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 d2 7b 03 00 00 00 00 00 d2 7b 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 66 5e 15 00 00 00 00 00 da a0 0a 00 00 00 00 00 40 ff 1f 00 00 00 00 00 20 dd 0a 00 00 00 00 00 ea 1d d9 50 00 00 00 00 9c 13 4a 16 00 00 00 00 93 f1 5f 0d 00 00 00 00 8e 70 d1 00 00 00 00 00 52 93 00 00 80 b1 00 00 a7 64 04 00 c3 e5 05 00 da a0 0a 00 fb 7e 15 00 20 dd 0a 00 d2 7a 29 00 5a 29 01 00 8a d1 0f 00 00 00 00 00 dd 74 19 00 89 51 04	.....;.~`.).....Zb ..... .....%.....` .....L.....{..... {.....f^.....@..... .....P.... ..J....._.....p.....R..... ...d.....~.. ....z).Z).. .....t...Q.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.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 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	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADCE.tmp.dmp	unknown	120	03 00 00 00 94 00 00 00 08 07 00 00 04 00 00 00 7c 18 00 00 a8 07 00 00 0e 00 00 00 24 00 00 00 24 20 00 00 05 00 00 00 04 01 00 00 06 35 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 0c 9c 00 00 15 00 00 00 ec 01 00 00 48 20 00 00 16 00 00 00 98 00 00 00 34 22 00 00	.....|.....$...$ .....5.....`... ....8.....T.....# .....H .....4"..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 34 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.4.8.0.<./.P.i.d.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 39 00 31 00 37 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.9.9.1.7.2.<./.U.p.t.i.m.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 35 00 38 00 34 00 38 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.6.5.5.8.4.8.9.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.3.7.2.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 38 00 37 00 37 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.2.8.7.7.8.2.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 38 00 39 00 34 00 30 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.2.6.8.9.4.0.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 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 50 00 61 00 67 00 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.>.2.4.1.8.0.8.<./.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.3.9.7.4.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 30 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.3.6.0.6.4.<./.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 30 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.6.0.6.4.<./.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 37 00 34 00 30 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.5.7.4.0.8.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 30 00 37 00 37 00 38 00 38 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.>.7.0.7.7.8.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 37 00 34 00 30 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.6.5.7.4.0.8.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 38 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.8.0.0.<./.P.i.d.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 39 00 39 00 30 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.>.9.9.9.0.1.<./.U.p.t.i.m.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 39 00 32 00 34 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.7.1.9.2.4.4.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 30 00 30 00 37 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.>.2.0.0.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 34 00 32 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.9.4.2.7.2.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 39 00 33 00 34 00 35 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.9.3.4.5.2.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.1.5.2.2.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 33 00 36 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.>.1.0.7.3.6.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 35 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.3.5.4.4.<./.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 32 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.3.2.7.2.<./.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 37 00 38 00 33 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.9.7.8.3.6.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 38 00 36 00 35 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.9.8.6.5.6.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 37 00 38 00 33 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.1.9.7.8.3.6.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 63 00 73 00 68 00 69 00 68 00 79 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.>.c.s.h.i.h.y.,. .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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 63 00 73 00 68 00 69 00 68 00 79 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.>.c.s.h.i.h.y.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 37 00 36 00 31 00 37 00 36 00 37 00 34 00 35 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.>.1.5.7.6.1.7.6.7.4.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 33 00 35 00 3a 00 33 00 32 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s..B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.5.-.0.5.T.0.4.:.3.5.:.3.2.Z.".>.	success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 33 00 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 34 00 38 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 35 00 33 00 33 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 35 00 33 00 33 00 34 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.3.8.". .P.I.D.=.".5.4.8.0.". .U.p.t.i.m.e.M.S.=.".4.5.3.3. 4.". .T.i.m.e.S.i.n.c.e.C.r.e. a.t.i.o.n.M.S.=.".4.5.3.3.4.". .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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 38 00 66 00 66 00 39 00 66 00 66 00 64 00 2d 00 33 00 64 00 35 00 66 00 2d 00 34 00 39 00 35 00 63 00 2d 00 62 00 33 00 66 00 39 00 2d 00 36 00 35 00 62 00 30 00 65 00 31 00 31 00 32 00 65 00 62 00 64 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.f.8.f.f.9.f.f.d.-.3.d.5.f.-.4.9.5.c.-.b.3.f.9.-.6.5.b.0.e.1.1.2.e.b.d.a.<./.G.u.i.d.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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 33 00 35 00 3a 00 33 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.0.5.T.0.4.:.3.5.:.3.2.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER58E4.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	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8C49.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	6F6D497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6D43D1	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 37 77 01 00 00 00 90 58 3B 77 0A 00 00 00 0A 00 00 00 14 FB A7 00 00 00 A8 00 00 00 00 00 0A 00 00 00 D0 FA A7 00 00 00 00 00 6C FB A7 00 F0 17 31 77 97 81 15 39 FE FF FF FF 38 FB A7 00 D1 86 2F 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	6F6F1FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: 7032 Parent PID: 5800

General

Start time:	21:34:35
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:	0x10d0000
File size:	61952 bytes

MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 7100 Parent PID: 5800

General

Start time:	21:34:35
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:	0x10d0000
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: 00000013.00000002.494169228.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 7136 Parent PID: 5800

General

Start time:	21:34:35
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:	0x10d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 776 Parent PID: 5800

General

Start time:	21:34:36
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:	0x10d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6232 Parent PID: 5800

General

Start time:	21:34:36
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:	0x10d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 6316 Parent PID: 5800

General

Start time:	21:34:40
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5800 -s 580
Imagebase:	0x1200000
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	6F6E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD73C.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE074.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE074.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_c2da78b9b5d245e5b326a942776d6525a82eddd_160cf2be_18f7e777	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_c2da78b9b5d245e5b326a942776d6525a82eddd_160cf2be_18f7e777\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp	success or wait	1	6F6D497A	unknown
unknown	success or wait	1	6F6D497A	unknown
unknown	success or wait	1	6F6D497A	unknown
unknown	success or wait	1	6F6D497A	unknown
unknown	success or wait	1	6F6D497A	unknown
unknown	success or wait	1	6F6D497A	unknown
unknown	success or wait	1	6F6D497A	unknown
unknown	success or wait	1	6F6D497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	32			success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	6			success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	1420			success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	716			success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	168			success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	20			success or wait	17	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	4964			success or wait	16	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	644			success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	4			success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	716			success or wait	3	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	48			success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	4			success or wait	32	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	32			success or wait	32	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	120			success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	62			success or wait	2	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	668			success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	9142			success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF47C.tmp.dmp	unknown	120			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	78			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	38			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	44			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	82			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	82			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	62			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	134			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	44			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	72			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	64			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	34			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	46			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	30			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	72			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	90			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	46			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	82			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	52			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	44			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	86			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	70			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	74			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	96			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	80			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	114			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	98			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	124			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	108			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	76			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	92			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	72			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	46			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	30			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	30			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	70			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	90			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	48			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	78			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	52			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	44			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	90			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	74			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	76			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	100			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	82			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	114			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	98			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	124			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	108			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	78			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	94			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	74			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	46			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	42			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	32			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	42			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	38			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	52			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	9	6F6D497A	unknown
unknown	unknown	2			success or wait	18	6F6D497A	unknown
unknown	unknown	76			success or wait	9	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	38			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	6	6F6D497A	unknown
unknown	unknown	2			success or wait	12	6F6D497A	unknown
unknown	unknown	96			success or wait	6	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	38			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	94			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	106			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	96			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	120			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	82			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	102			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	68			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	34			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	96			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	36			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	24			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	3	6F6D497A	unknown
unknown	unknown	2			success or wait	6	6F6D497A	unknown
unknown	unknown	46			success or wait	3	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	26			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	100			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	266			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	20			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	38			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	38			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	98			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	98			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4694			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	22			success or wait	157	6F6D497A	unknown
unknown	unknown	44			success or wait	1	6F6D497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6F36BF	unknown

Analysis Process: WerFault.exe PID: 4260 Parent PID: 7032

General

Start time:	21:35:41
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7032 -s 752
Imagebase:	0x1200000
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	6F6E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE312.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE312.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF11D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF11D.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4D7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF4D7.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_e567c4b21b84c537cff2f3cec9da318e31a88c0_82810a17_10f80b1c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F6D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_e567c4b21b84c537cff2f3cec9da318e31a88c0_82810a17_10f80b1c\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F6D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
unknown	success or wait	1	6F6D497A	unknown
unknown	success or wait	1	6F6D497A	unknown
unknown	success or wait	1	6F6D497A	unknown
unknown	success or wait	1	6F6D4BEF	unknown
unknown	success or wait	1	6F6D4BEF	unknown
unknown	success or wait	1	6F6D4BEF	unknown
unknown	success or wait	1	6F6D4BEF	unknown
unknown	success or wait	1	6F6D4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	32			success or wait	1	6F6D497A	unknown
unknown	unknown	6			success or wait	1	6F6D497A	unknown
unknown	unknown	1420			success or wait	1	6F6D497A	unknown
unknown	unknown	716			success or wait	1	6F6D497A	unknown
unknown	unknown	168			success or wait	1	6F6D497A	unknown
unknown	unknown	20			success or wait	15	6F6D497A	unknown
unknown	unknown	5204			success or wait	14	6F6D497A	unknown
unknown	unknown	852			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	3	6F6D497A	unknown
unknown	unknown	716			success or wait	3	6F6D497A	unknown
unknown	unknown	48			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	53	6F6D497A	unknown
unknown	unknown	30			success or wait	53	6F6D497A	unknown
unknown	unknown	752			success or wait	1	6F6D497A	unknown
unknown	unknown	10666			success or wait	1	6F6D497A	unknown
unknown	unknown	108			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	78			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	38			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	44			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	82			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	82			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	62			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	134			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	44			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	72			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	64			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	34			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	46			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	30			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	70			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	90			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	44			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	82			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	52			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	44			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	88			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	72			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	74			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	96			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	80			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	114			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	98			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	124			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	108			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	76			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	92			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	72			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	46			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	30			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	30			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	86			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	90			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	46			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	82			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	52			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	44			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	86			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	56			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	74			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	96			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	76			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	114			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	90			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	124			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	100			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	72			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	92			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	5	6F6D497A	unknown
unknown	unknown	68			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	4	6F6D497A	unknown
unknown	unknown	46			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	3	6F6D497A	unknown
unknown	unknown	42			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	32			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	42			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	38			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	62			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	8	6F6D497A	unknown
unknown	unknown	2			success or wait	16	6F6D497A	unknown
unknown	unknown	74			success or wait	8	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	38			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	6	6F6D497A	unknown
unknown	unknown	2			success or wait	12	6F6D497A	unknown
unknown	unknown	96			success or wait	6	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	38			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	94			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	106			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	96			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	120			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	82			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	102			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	68			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	34			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	96			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	36			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	24			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	3	6F6D497A	unknown
unknown	unknown	2			success or wait	6	6F6D497A	unknown
unknown	unknown	46			success or wait	3	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	26			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	100			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	266			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	20			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	38			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	38			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	98			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	2	6F6D497A	unknown
unknown	unknown	98			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4			success or wait	1	6F6D497A	unknown
unknown	unknown	40			success or wait	1	6F6D497A	unknown
unknown	unknown	4679			success or wait	1	6F6D497A	unknown
unknown	unknown	2			success or wait	1	6F6D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	22			success or wait	184	6F6D497A	unknown
unknown	unknown	48			success or wait	1	6F6D497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6F36BF	unknown
\REGISTRY\A\{2ab8b7f5-774d-5cd6-0724-4d431bd87296}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6D43D1	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 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	74 03 00 C0 01 00 00 00 00 00 00 00 79 8E 37 77 01 00 00 00 90 58 3B 77 B1 E1 FC FF 0A 00 00 00 E4 F9 07 01 00 00 08 01 00 00 00 00 0A 00 00 00 A0 F9 07 01 00 00 00 00 3C FA 07 01 F0 17 31 77 95 E6 9F 40 FE FF FF FF 08 FA 07 01 D1 86 2F 77	success or wait	1	6F6F1FE8	RegSetValueExW

Disassembly

Code Analysis