ID: 379667
Sample Name: ghost.dll
Cookbook: default.jbs
Time: 06:11:22
Date: 01/04/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright Joe Security LLC 2021

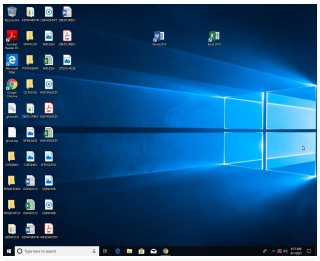
Analysis Report ghost.dll

Overview

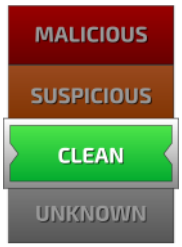
General Information

Sample Name:	ghost.dll
Analysis ID:	379667
MD5:	3b491b7d2e499a..
SHA1:	842627191fe181f..
SHA256:	b0bc056257f5bee.
Infos:	

Most interesting Screenshot:



Detection

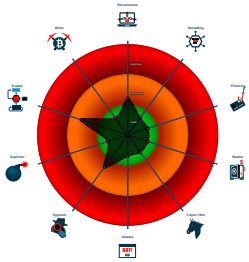


Score:	6
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Checks if the current process is bein…
- Contains functionality to check if a d…
- Contains functionality to query CPU …
- Creates a process in suspended mo…
- Detected potential crypto function
- Found large amount of non-executed…
- Monitors certain registry keys / valu…
- One or more processes crash
- PE file contains strange resources
- Queries the volume information (nam…
- Uses 32bit PE files
- Uses code obfuscation techniques (…

Classification



Analysis Advice

Sample crashes during execution, try analyze it on another analysis machine

Sample is a C# Dll, sample needs to be analyzed in a .Net context

Startup

- **System is w10x64**
- loaddll32.exe (PID: 6984 cmdline: loaddll32.exe 'C:\Users\user\Desktop\ghost.dll' MD5: 0A44868D26BC4DA6847ED7EF6AAFD427)
  - cmd.exe (PID: 6992 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\ghost.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7012 cmdline: rundll32.exe 'C:\Users\user\Desktop\ghost.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7000 cmdline: rundll32.exe C:\Users\user\Desktop\ghost.dll,?addZombie@ghostlib@@YAXU_clientData@1@@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7112 cmdline: rundll32.exe C:\Users\user\Desktop\ghost.dll,?deleteZombie@ghostlib@@YAXH@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6424 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7112 -s 1028 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6384 cmdline: rundll32.exe C:\Users\user\Desktop\ghost.dll,?getZombieCount@ghostlib@@YAHXZ MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5236 cmdline: rundll32.exe C:\Users\user\Desktop\ghost.dll,?getZombieData@ghostlib@@YAAAU_clientData@1@H@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6008 cmdline: rundll32.exe C:\Users\user\Desktop\ghost.dll,?getZombieIndex@ghostlib@@YAHI@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6664 cmdline: rundll32.exe C:\Users\user\Desktop\ghost.dll,?parseZombie@ghostlib@@YAXIHPAD@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6728 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6664 -s 1028 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6828 cmdline: rundll32.exe C:\Users\user\Desktop\ghost.dll,?updateZombieConnection@ghostlib@@YAXHI@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6900 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6828 -s 1028 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6696 cmdline: rundll32.exe 'C:\Users\user\Desktop\ghost.dll',?addZombie@ghostlib@@YAXU_clientData@1@@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7056 cmdline: rundll32.exe 'C:\Users\user\Desktop\ghost.dll',?deleteZombie@ghostlib@@YAXH@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6360 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7056 -s 1028 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 1724 cmdline: rundll32.exe 'C:\Users\user\Desktop\ghost.dll',?getZombieCount@ghostlib@@YAHXZ MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6152 cmdline: rundll32.exe 'C:\Users\user\Desktop\ghost.dll',?getZombieData@ghostlib@@YAAAU_clientData@1@H@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1864 cmdline: rundll32.exe 'C:\Users\user\Desktop\ghost.dll',?getZombieIndex@ghostlib@@YAHI@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Copyright Joe Security LLC 2021

Malware Configuration

No configs have been found

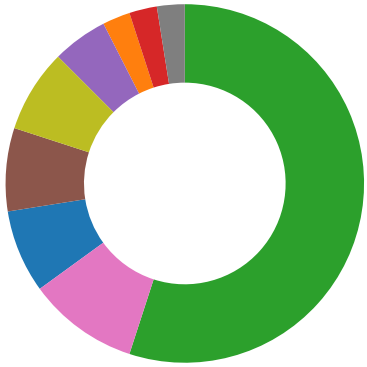
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Networking
- 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

Click to jump to signature section

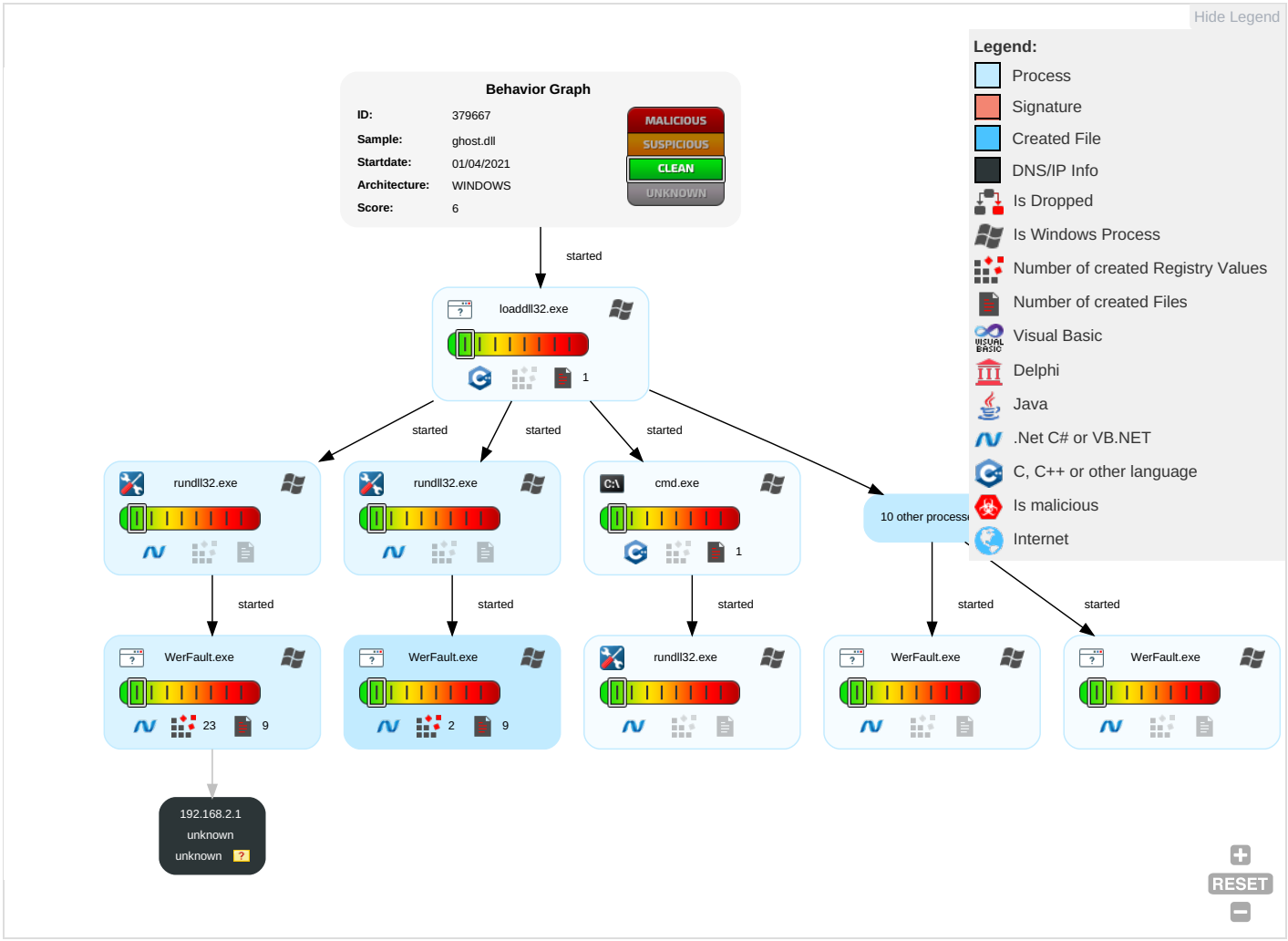
There are no malicious signatures, click here to show all signatures.

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	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rundll32 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Security Software Discovery 2 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)	Virtualization/Sandbox Evasion 1 1	NTDS	Virtualization/Sandbox Evasion 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1	LSA Secrets	System Information Discovery 2 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

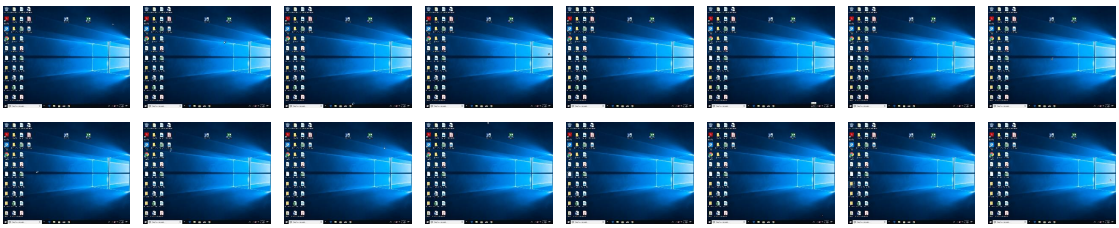
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ghost.dll	0%	Virustotal		Browse
ghost.dll	0%	Metadefender		Browse
ghost.dll	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

No contacted domains info

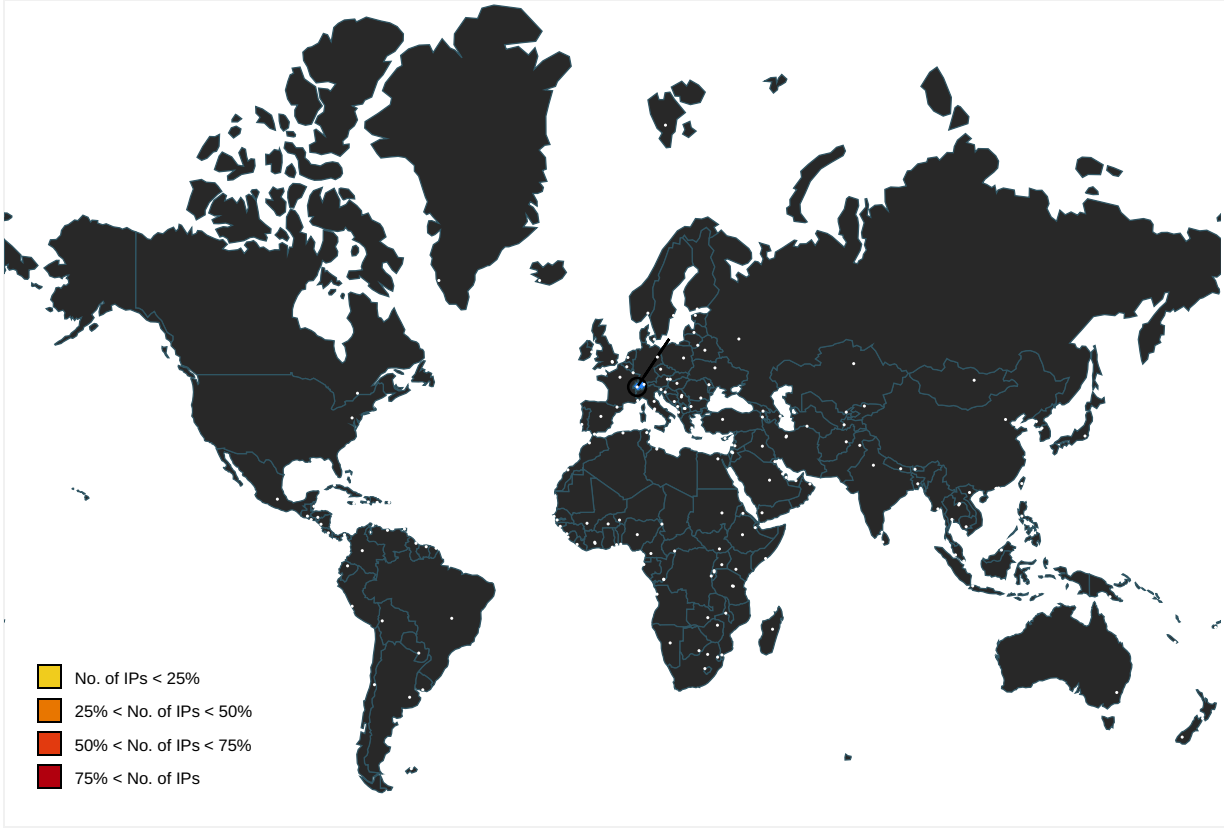
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 0000000A.00000003.353479613.0000000004E10000.00000004.00000001.sdmp, WerFault.exe, 00000011.00000003.379994838.000000054D0000.00000004.00000001.sdmp, WerFault.exe, 00000014.00000003.391702222.0000000004D30000.00000004.00000001.sdmp, WerFault.exe, 0000001B.00000003.409135731.0000000005100000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 0000000A.00000003.353479613.0000000004E10000.00000004.00000001.sdmp, WerFault.exe, 00000011.00000003.379994838.000000054D0000.00000004.00000001.sdmp, WerFault.exe, 00000014.00000003.391702222.0000000004D30000.00000004.00000001.sdmp, WerFault.exe, 0000001B.00000003.409135731.0000000005100000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 0000000A.00000003.353479613.0000000004E10000.00000004.00000001.sdmp, WerFault.exe, 00000011.00000003.379994838.000000054D0000.00000004.00000001.sdmp, WerFault.exe, 00000014.00000003.391702222.0000000004D30000.00000004.00000001.sdmp, WerFault.exe, 0000001B.00000003.409135731.0000000005100000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 0000000A.00000003.353479613.0000000004E10000.00000004.00000001.sdmp, WerFault.exe, 00000011.00000003.379994838.000000054D0000.00000004.00000001.sdmp, WerFault.exe, 00000014.00000003.391702222.0000000004D30000.00000004.00000001.sdmp, WerFault.exe, 0000001B.00000003.409135731.0000000005100000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddressxhttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 0000000A.00000003.353479613.0000000004E10000.00000004.00000001.sdmp, WerFault.exe, 00000011.00000003.379994838.000000054D0000.00000004.00000001.sdmp, WerFault.exe, 00000014.00000003.391702222.0000000004D30000.00000004.00000001.sdmp, WerFault.exe, 0000001B.00000003.409135731.0000000005100000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 0000000A.00000003.353479613.0000000004E10000.00000004.00000001.sdmp, WerFault.exe, 00000011.00000003.379994838.000000054D0000.00000004.00000001.sdmp, WerFault.exe, 00000014.00000003.391702222.0000000004D30000.00000004.00000001.sdmp, WerFault.exe, 0000001B.00000003.409135731.0000000005100000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	WerFault.exe, 0000000A.0000000 3.353479613.0000000004E10000.0 0000004.00000001.sdmp, WerFault.exe, 00000011.00000003.379994838.00000 000054D0000.00000004.00000001. sdmp, WerFault.exe, 00000014.0 0000003.391702222.0000000004D3 0000.00000004.00000001.sdmp, W erFault.exe, 0000001B.00000003 .409135731.0000000005100000.00 000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	WerFault.exe, 0000000A.0000000 3.353479613.0000000004E10000.0 0000004.00000001.sdmp, WerFault.exe, 00000011.00000003.379994838.00000 000054D0000.00000004.00000001. sdmp, WerFault.exe, 00000014.0 0000003.391702222.0000000004D3 0000.00000004.00000001.sdmp, W erFault.exe, 0000001B.00000003 .409135731.0000000005100000.00 000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 0000000A.0000000 3.353479613.0000000004E10000.0 0000004.00000001.sdmp, WerFault.exe, 00000011.00000003.379994838.00000 000054D0000.00000004.00000001. sdmp, WerFault.exe, 00000014.0 0000003.391702222.0000000004D3 0000.00000004.00000001.sdmp, W erFault.exe, 0000001B.00000003 .409135731.0000000005100000.00 000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprinthttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000000A.0000000 3.353479613.0000000004E10000.0 0000004.00000001.sdmp, WerFault.exe, 00000011.00000003.379994838.00000 000054D0000.00000004.00000001. sdmp, WerFault.exe, 00000014.0 0000003.391702222.0000000004D3 0000.00000004.00000001.sdmp, W erFault.exe, 0000001B.00000003 .409135731.0000000005100000.00 000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	WerFault.exe, 0000000A.0000000 3.353479613.0000000004E10000.0 0000004.00000001.sdmp, WerFault.exe, 00000011.00000003.379994838.00000 000054D0000.00000004.00000001. sdmp, WerFault.exe, 00000014.0 0000003.391702222.0000000004D3 0000.00000004.00000001.sdmp, W erFault.exe, 0000001B.00000003 .409135731.0000000005100000.00 000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddresszhttp://schemas.xmlsoap.org/ws/20	WerFault.exe, 0000000A.0000000 3.353479613.0000000004E10000.0 0000004.00000001.sdmp, WerFault.exe, 00000011.00000003.379994838.00000 000054D0000.00000004.00000001. sdmp, WerFault.exe, 00000014.0 0000003.391702222.0000000004D3 0000.00000004.00000001.sdmp, W erFault.exe, 0000001B.00000003 .409135731.0000000005100000.00 000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcoderhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000000A.0000000 3.353479613.0000000004E10000.0 0000004.00000001.sdmp, WerFault.exe, 00000011.00000003.379994838.00000 000054D0000.00000004.00000001. sdmp, WerFault.exe, 00000014.0 0000003.391702222.0000000004D3 0000.00000004.00000001.sdmp, W erFault.exe, 0000001B.00000003 .409135731.0000000005100000.00 000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 0000000A.00000003.353479613.0000000004E10000.00000004.00000001.sdmp, WerFault.exe, 00000011.00000003.379994838.00000000054D0000.00000004.00000001.sdmp, WerFault.exe, 00000014.00000003.391702222.0000000004D30000.00000004.00000001.sdmp, WerFault.exe, 0000001B.00000003.409135731.0000000005100000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	379667
Start date:	01.04.2021
Start time:	06:11:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ghost.dll
Cookbook file name:	default.jbs

Copyright Joe Security LLC 2021

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:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean6.winDLL@33/17@0/1
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 14.1% (good quality ratio 13.4%) • Quality average: 71.2% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 20.82.209.183, 23.218.209.198, 92.122.145.220, 93.184.221.240, 168.61.161.212, 104.43.139.144, 52.147.198.201, 13.88.21.125, 92.122.213.194, 92.122.213.247, 2.20.142.209, 2.20.142.210, 52.155.217.156, 20.54.26.129, 23.218.208.56 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.net, 2-01-3cf7-0009.cdx.cedexis.net, store-images.s-microsoft.com-c.edgekey.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, storeedgefd.xbetservices.akadns.net, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, cs11.wpc.v0cdn.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, prod.fs.microsoft.com.akadns.net, storeedgefd.dsx.mp.microsoft.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, download.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Execution Graph export aborted for target WerFault.exe, PID 6360 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 5236 because there are no executed function • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:12:34	API Interceptor	4x Sleep call for process: WerFault.exe modified
06:12:37	API Interceptor	2x Sleep call for process: loaddll32.exe modified

Copyright Joe Security LLC 2021

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_79b71d382ebf0d012f2cc7d36f633e8f07b7640_82810a17_1aad3cd9\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13370
Entropy (8bit):	3.7677534214235533
Encrypted:	false
SSDEEP:	192:73Gi40oXh5HBUZMX4jed+Fb/u7sYS274ItCca:TGi+X/BUZMX4jek/u7sYX4ItCca
MD5:	7D3930D7BD6A0E8BD136A9ADBBAB0A71
SHA1:	6CBA5C28762834FE93E053D64B5A375BDA9E2551
SHA-256:	F689098217BC7B19AD85A01C44847640C45B8ADDC57404F7A2FD54B5D4A3E662
SHA-512:	9D1FD2E5A7E64CB0C671702E09FA1CC30DB5899603A961A3AD99A184494BCD7ACC301525FCAC4A088BA1818272B2622E7C94B8B6C697E823AE1D8B2AAEA046C6
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.1.7.5.6.3.5.8.6.3.0.5.1.5.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.1.7.5.6.3.7.8.0.3.6.6.6.6.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.8.c.5.0.0.8.9.-.9.f.5.c.-.4.9.9.b.-.a.2.6.0.-.2.2.0.7.4.4.e.1.2.3.9.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.c.2.4.5.1.6.b.-.4.c.0.d.-.4.c.1.3.-.9.7.d.7.-.9.e.8.4.7.0.a.3.8.d.8.f.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.a.c.-.0.0.0.1.-.0.0.1.7.-.1.e.f.4.-.0.8.a.e.f.8.2.6.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_e8ec31b4b32c25a646f8b3a58a24f343d9e92b6_82810a17_18814dd1\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13372
Entropy (8bit):	3.767157863748433
Encrypted:	false
SSDEEP:	192:VuMih0oXDYHBUZMX4jed+Fb/u7sYS274ItCc7:ViPXkBUZMX4jek/u7sYX4ItCc7
MD5:	342E40136261B63604A7C631D9DAF0EC
SHA1:	55586C6001D8A597ECF4B3F73824ADA07F1B4DBD
SHA-256:	85F5C750586299779ED1736589620AD1F9B9394D1140A00FF526C21403F13BB5
SHA-512:	39AC0FA8968F628B23A02C62429DA16002AF9C4852E4F616C7250E3C0936405180F7A4AB4EF6FFA728FB35B8D51CBAF47B0AB317E7D5DB157F6492FDD4389EE
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_e8ec31b4b32c25a646f8b3a58a24f343d9e92b6_82810a17_18814dd1\Report.wer	
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.1.7.5.6.3.6.3.7.7.1.1.1.8.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.1.7.5.6.3.8.2.0.2.1.0.2.6.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.a.7.c.2.1.9.c.-.b.c.5.3.-.4.0.3.3.-.a.9.8.1.-.7.2.c.5.e.8.a.6.f.e.3.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.9.5.9.4.b.9.c.-.e.9.7.c.-.4.9.7.1.-.a.c.0.2.-.b.5.7.5.6.0.9.a.3.2.d.0.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.9.0.-.0.0.0.1.-.0.0.1.7.-.9.a.8.6.-.4.3.b.0.f.8.2.6.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_e8ec31b4b32c25a646f8b3a58a24f343d9e92b6_82810a17_1940d40d\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13370
Entropy (8bit):	3.766270257627739
Encrypted:	false
SSDEEP:	192:Lwib0oX/YHBUZMX4jed+Fb/u7sYS274ItCc6:MiFX4BUZMX4jek/u7sYX4ItCc6
MD5:	9E51C80B5E987727B14429D6CCB80E38
SHA1:	B46A13AA46B8E0997EBDDED2A5A74BB94D452A80
SHA-256:	05A67F835456185E55B38ABBF6772385EFF8034113C6A0F7E4B8A660F02DABA3
SHA-512:	210B8805B05DF6A372782BAD96460CBD2E8F4270D28E574349F4574A19950C78A12347C8FCB09AA8E7BD6531143B02C3D58272E02D33A2D470810A600FE970C6
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.1.7.5.6.3.4.2.7.3.9.9.6.0.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.1.7.5.6.3.5.2.2.8.6.8.0.3.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.9.f.5.6.a.7.c.-.1.d.d.3.-.4.6.5.5.-.8.d.8.a.-.0.0.0.b.e.0.2.4.f.b.a.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.4.6.2.8.4.9.c.-.5.8.7.7.-.4.a.0.e.-.9.3.b.1.-.c.6.7.6.e.b.4.5.4.3.d.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.c.8.-.0.0.0.1.-.0.0.1.7.-.0.4.6.9.-.c.a.a.3.f.8.2.6.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_facd47adbece4b362bc62fffc58409335218397_82810a17_1a111f1f\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	13368
Entropy (8bit):	3.767270415817665
Encrypted:	false
SSDEEP:	192:BWrtiN0oXcPHBUZMX4jed+Fb/u7sYS274ItCci:atiDXsBUZMX4jek/u7sYX4ItCci
MD5:	325A9CCCAA6E6EE482E550BC009A9274
SHA1:	A3CE9BE9D4B8585ECDA760F8FE4414E25272A55D
SHA-256:	3EBCF899FEE83607E76D73F5B72F619C8E612B2BC615B6D5C6EBE356D625015C
SHA-512:	F541E11B0D36D8F7250E1810AC925B72A80004D734C716FF13BA579A8893B9F55B9E73B983E1A32C3EAD6FA1B19FC48B30DE9580DCF6DE9B60D872EA31B931E1
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.1.7.5.6.3.5.5.0.2.1.1.6.2.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.1.7.5.6.3.7.1.2.7.1.0.7.7.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.0.4.b.1.4.a.5.-.1.2.9.4.-.4.c.6.a.-.b.f.6.5.-.2.5.5.2.1.f.f.0.c.b.8.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.e.3.2.0.9.5.4.-.c.b.9.f.-.4.9.7.7.-.a.4.2.f.-.9.4.e.3.e.b.d.8.6.4.0.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.0.8.-.0.0.0.1.-.0.0.1.7.-.9.e.5.0.-.0.6.a.c.f.8.2.6.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1C32.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):	8346
Entropy (8bit):	3.690932145842804
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi5M6eh0W6Yx36HgmfZxfScCpra89bwOsfnzm:RrlsNiy6eh0W6YR6HgmfvfSHwNfq
MD5:	E4DE03CCD0B5FF4FC656800F9542235D
SHA1:	E576DE7C6266A497EDB6739F4F7E5FB0FC6284B6
SHA-256:	217E29A8C08CAF826E8901DDD8AACB29088100FD4C4FF66989791720B762D98C
SHA-512:	495DE7C52990451EB9C44A95C0E586F2DBCE69E30BECDCEAB28AD28991B16FF9496FC8C202C4F9B324565CA857FC4CCCDB5F7754947FEA79BA81ACD1D20E5CA
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1C32.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.5.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2377.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4752
Entropy (8bit):	4.471287003032959
Encrypted:	false
SSDEEP:	48:cvIwSD8zsjJgtWI9MHSWSC8Bjs8fm8M4JCdsuFVUGVn+q8vosc4SrSrd:uITf9zTSN9RJgVKaDWrd
MD5:	CF8CDA3E158EA847EB6810868C045B48
SHA1:	0853F7F22D9D665C35C7FD5E75A8D8A1A702290D
SHA-256:	394364AC53AECCA1107A02B193848CC00C956E6A6BA4800F5347A939D4759D3E
SHA-512:	3C70B081F3EE8A08C7959895C052EA89BB8A658F8FC4B227FE7C0D811D2A57B756B7B7AE81C4D3AC7B81E9F809CB0029BBE84027E245EE98390811FAF6D1DF5 3
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="927263" />.. <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\WER37B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4750
Entropy (8bit):	4.469693436591577
Encrypted:	false
SSDEEP:	48:cvIwSD8zsjJgtWI9MHSWSC8BNs8fm8M4JCdsRFPm+q8vosG4SrSZd:uITf9zTSNbRJpmKoDWZd
MD5:	DC4BB8356DAC3D04CF69BA767A05F15E
SHA1:	A769C873321473CB8A5DDE407FDE1F6D9763204F
SHA-256:	67E3B50060CD6EF174D5DF435505FB70ACCDEA8199B2F8453486D1E019BEB915
SHA-512:	09CD561251F5513C7E7A60E2F59FD4F6274453E5F176ED2FB3AA1430F7101C72D3138A99A88F899C7661B783B666C27A982DC9D5F246F2F03EB3F44749F570DF
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="927263" />.. <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\WERA77E.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Apr 1 13:12:25 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	125541
Entropy (8bit):	3.638146182456151
Encrypted:	false
SSDEEP:	1536:Ev303oGF4HwNaCgUziUznkwrOD4m6oQin7vTSD7m:Ev04HwUCgUnkaODE/i7vTSDa
MD5:	2079D6FF192E666CAF05CDDDDD13D158
SHA1:	31D41C20FD18509FCAF8FC00FD5B485092D49E98
SHA-256:	E4B5A6559CC96998869520B652F8EC96A6C52B9D4488901D6233E7FF6EA83917
SHA-512:	1521711B6465398FBD0A61490F634DC9D01442C3607BDB08B8FA5BD8D228A225875D856276221B1527D37730E8AD5ECDABBA35A15ED2834373A688D3F166BC7
Malicious:	false
Preview:	MDMP..... .....e`.....U.....B.....!.....GenuineIntelW.....T.....e`.....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\WERB2AB.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):	8352
Entropy (8bit):	3.6902693237762882
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNigTA6TTA6YZg6KSugmfZxfScCprd89bIRsflYm:RrlsNiT6TTA6Yu62gmfvfS+IKff
MD5:	CEE5A1B09D5863349E7288C3DCFCAB29
SHA1:	77C46E74DA74DEB5996AED8123EF8EE96005243C
SHA-256:	3A903F7BE6DDD11E82BBC9FDE246C98D64104CA0B19879F31BB6CA9E999CDCE9
SHA-512:	F3F32D447A73A1212760B3693A8AF2A4957B766FA075EA912131B67C8524458091B3D7DDA43827BEE7BA80ADD45DCD4F6137DFF970161B4A9CB6D52E0C04A96
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....</.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.1.2.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7EC.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4752
Entropy (8bit):	4.471403521697566
Encrypted:	false
SSDEEP:	48:cvIwSD8zsjJgtWI9MHSWSC8BLs8fm8M4JCdsuFkH+q8vos24SrSNd:uITf9zTSNFRJvKoDWNd
MD5:	8E53B2695119F54C1A5D6147E27EB3D3
SHA1:	6CBFB1E3638857574729C38206D0AADBF2E2247E
SHA-256:	B1CCE7426F4215426BA49A0A3CB7012604552D8A36825DFD13089C96ACD99E1E
SHA-512:	D076D7272AD10BAAA2F75CAD21F990B89472B4968CF502677430A52624AA7EAF9B6DF6770141B85DE19444B475CD35B4846C29DA11852B824A915F9C38F39233
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="927263" />.. <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\WERD778.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Apr 1 13:12:38 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	133546
Entropy (8bit):	3.5280066835788473
Encrypted:	false
SSDEEP:	1536:cS303oGFm0NaCgUziUVBQOBLa9FqodEj6RSNc7JuCc:cS0m0UCgUTQ6MFq6q6B0
MD5:	DEC79345D10AFCEF9997E87304917B6B
SHA1:	A1BFDF920B5AB09CC044188B7C12F43599EAD4F3
SHA-256:	CA45A664F8C191D3AC70B839BF0636FEBE06D0AE7A46765A9701D1A0E75E6E15
SHA-512:	5C73795567CE5678B5CA6C95F2315072F23616E16BFF732947191F766457DD22DB11BF55D69589223AD66CE2A1398948DEF299321BFB45A0E5B76D61C7378448
Malicious:	false
Preview:	MDMP..... .....e`.....U.....B.....!.....GenuineIntelW.....T.....e`.....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\WERE591.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Apr 1 13:12:43 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	126894
Entropy (8bit):	3.6358525044245487
Encrypted:	false
SSDEEP:	1536:j303oGFbNaCgUziUAfbF9BmqKzpVLV6lr9:j0bUCgUMfbz96pVslh

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE591.tmp.dmp	
MD5:	DDC3DFCB8E66F053F3F448EED82A808A
SHA1:	ECFDA5EC3B3E57B04986F2A0222357345B57B51B
SHA-256:	659ED988465F00110A0D0CDFB4FD129816D105227228503748190A4FD070B032
SHA-512:	D1ABDBBFF0284C4B09B2E816202AEFCCE033FCE3F0D9FAEEEA0717A2E393D6EB879AF2F3D3DEA0FE329D13F2DE02863C7FC67C155710A60F01083B71273648FD
Malicious:	false
Preview:	MDMP..... .....e`.....U.....B.....!.....GenuineIntelW.....T.....e`.....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\WERE61F.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):	8362
Entropy (8bit):	3.6928334554446987
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiPL6CA6YZ56nggmfZx2ScCprl+89bTRssfv2RBm:RrlsNiT6CA6Yn6nggmfv2SJTR/fvm8
MD5:	677C5336FB3B74D89A2661885F16DB88
SHA1:	184B8185173351B14524FF1648757BEE92C54772
SHA-256:	42B6D9F9DFAB8CF921D0E65CE26FA1A88C6DD14FACDE976531F157FF16F05790
SHA-512:	1A211A3CC598A126544B50719C232388EA3BDB76AD5D070165AD3F8A337E1DB47C961CA5382075262CA9E80AD09FA90C8A3E972D7352FBFD66C965B2C054A97
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.>.6.6.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBFC.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4750
Entropy (8bit):	4.469066105228834
Encrypted:	false
SSDEEP:	48:cvIwSD8zsjJgtWI9MHSWSC8Bw8fm8M4JCdsPF9Fo+q8vosF4SrS9d:uITf9zTSNHJoKDDW9d
MD5:	BFBC23E0E7D91C1F002682B0159D9593
SHA1:	46B3D67AA96627280429ADBB0C5FDF40D057B3F1
SHA-256:	5B7E7314AD470F3D9C0E2C1BC64F7AC3F9AAB7A82B5241A377F8882D54585AD7
SHA-512:	ADD6CB8578EF69BD02F324F535BEC4B0995DE7FAFE74375CADFA9121F9601466FF594FA2010AB064E0A06C9A19BB715A4C420D2F64681C846266B333968B8091
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="927263" />.. <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\WERF9A6.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Apr 1 13:12:51 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	127721
Entropy (8bit):	3.6026523644032626
Encrypted:	false
SSDEEP:	1536:2/303oGFANaCgUziUwPkw0bJVE6GwdhfLx8uyN:2/0AUCgUc875/FDO
MD5:	FB963CC00CB1A9BA165DBC49E7032995
SHA1:	A0C9954E8CE5460AD258A330BC33AAEE42529DAD
SHA-256:	668B321090435FC211A89535BD2148038A796D2FE66A5EA965166C0AE00C3ABA
SHA-512:	DBF4DAEBE16ADC2D3C8D0323E52DFA9CCF44AA6157BC042DD8DE9C0ECC9A053304AD1A0E5FCEFB0E92BBA7AC72700FF605CE2509612E9AF69D65F737BF95DD1E
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF9A6.tmp.dmp	
Preview:	MDMP..... .....e`.....U.....B.....!.....GenuineIntelW.....T.....e`.....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\WERFDCD.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):	8344
Entropy (8bit):	3.69246023156355
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiZj96B8t56Yx56HgmfZxMScCpru89bu+sfTBam:RrlsNiN96B8t56Y/6HgmfvMSDu9fTd
MD5:	30FD7B7976CAD8333D29D443E600553C
SHA1:	A0283CB315E130BC966FF04CFCCDA06AB23CB5AC
SHA-256:	8E711441A325D8BC6401A78D0B30924F641862E2221452FF1E26CB4A38DCA4BF
SHA-512:	9BA8181E0DC081E7FBAD8E8ADF4AB24A9D0A12B0C25EE0C59F6FDD79A49971D5BE213E660B16F14FAE580C515CC0A4F8C7AF529E0326800FBDBF3C7E0F7F5 61
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.>.6.8.2.8.<./.P.i.d.>.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\rundll32.exe.log	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.0050635535766075
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUy:Q3La/xwQ
MD5:	84CFDB4B995B1DBF543B26B86C863ADC
SHA1:	D2F47764908BF30036CF8248B9FF5541E2711FA2
SHA-256:	D8988D672D6915B46946B28C06AD8066C50041F6152A91D37FFA5CF129CC146B
SHA-512:	485F0ED45E13F00A93762CBF15B4B8F996553BAA021152FAE5ABA051E3736BCD3CA8F4328F0E6D9E3E1F910C96C4A9AE055331123EE08E3C2CE3A99AC2E177C E
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.903406593870656
TrID:	• Win32 Dynamic Link Library (generic) Net Framework (1011504/3) 50.14% • Win32 Dynamic Link Library (generic) (1002004/3) 49.67% • Generic Win/DOS Executable (2004/3) 0.10% • DOS Executable Generic (2002/1) 0.10% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	ghost.dll
File size:	346112
MD5:	3b491b7d2e499a6e99eb4041c519a966
SHA1:	842627191fe181fca8bc115507baab36f4b91654
SHA256:	b0bc056257f5bee8532b5978c082d9fd173eb07128aea13 af83938ca94ebe4dd

General

SHA512:	5655ff27161b79dccda10ac55933fbd12788534c6cec1a20a7583c04be4096facf8c1e8e7467d9542690f8f956b442286f9673ca7b83afaa36294171a70855d3
SSDEEP:	6144:lej8gAwB+9AhuU6tXqYXForMOQNTI+EUdHWA0ITmz56zXxzoEdq1a1o1G1HlrOUA:IC8gACxuU6tXqYXFsQNTI+EUdHWA0ITL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w.....nl.....a.....a.....a.....a.....Rich...

File Icon

Icon Hash:	41455554545445a2

Static PE Info

General

Entrypoint:	0x10009af8
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:	0x5A2C26B5 [Sat Dec 9 18:08:53 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	e46f6570fae44048af48d3411fda1e1f

Entrypoint Preview

Instruction
jmp dword ptr [1000A0E0h]
int3
int3
add esi, dword ptr [eax]
add al, 00h
arpl word ptr [eax], ax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
jnle 00007F06C4B8E125h
add byte ptr [eax], al
add al, 4Ah
sub al, 5Ah
jnle 00007F06C4B8E125h
add byte ptr [eax], al
add al, 28h
add byte ptr [eax], 00000000h
push es
jnle 00007F06C4B8E125h
add byte ptr [eax], al
add al, 7Fh
xor eax, dword ptr [eax]
add byte ptr [edx+ecx*2], al
jnle 00007F06C4B8E125h

Instruction
add byte ptr [eax], al
add al, 1Ah
pop eax
dec edx
sub byte ptr [eax+eax+00h], bl
push es
jnle 00007F06C4B8E125h
add byte ptr [eax], al
add al, 4Ah
jnle 00007F06C4B8E125h
add byte ptr [eax], al
add al, 1Eh
pop eax
dec edx
jnle 00007F06C4B8E125h
add byte ptr [eax], al
add al, 4Ah
pop ecx
pop ds
or al, 5Bh
pop ds
or al, 28h
sbb byte ptr [eax], al
add byte ptr [esi], al
jnle 00007F06C4B8E125h
add byte ptr [eax], al
add al, 16h
push esp
jnle 00007F06C4B8E125h
add byte ptr [eax], al
add al, 1Ah
pop eax
push ss
push esp
jnle 00007F06C4B8E125h
add byte ptr [eax], al
add al, 1Eh
pop eax
push ss
push esp
sub bh, bh
and eax, 1004A8DCh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Rich Headers

Programming Language:	• [LNK] VS2015 UPD1 build 23506 • [RES] VS2015 UPD1 build 23506 • [IMP] VS2008 build 21022 • [EXP] VS2015 UPD1 build 23506 • [C++] VS2015 UPD1 build 23506 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x49160	0x17e	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x492e0	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4d000	0xa598	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x58000	0x89c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xa290	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xa2e8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xa000	0xe8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0xa150	0x48	.rdata
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8b75	0x8c00	False	0.377566964286	data	5.42935217952	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xa000	0x3f970	0x3fa00	False	0.159480906189	data	5.6703775866	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4a000	0x14b4	0xc00	False	0.4296875	data	4.49929894955	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x4c000	0x44	0x200	False	0.095703125	Spectrum .TAP data "N " - BASIC program	0.334207160335	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4d000	0xa598	0xa600	False	0.0381447665663	data	3.36393796207	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x58000	0x89c	0xa00	False	0.726171875	data	6.02112075374	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4d270	0x3ed	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x4d660	0xea8	data	English	United States
RT_ICON	0x4e508	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x4edb0	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x4f318	0x398	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x4f6b0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x538d8	0x25a8	data	English	United States
RT_ICON	0x55e80	0x10a8	data	English	United States
RT_ICON	0x56f28	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_GROUP_ICON	0x57390	0x84	data	English	United States
RT_MANIFEST	0x57418	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
VCRUNTIME140.dll	__CxxQueryExceptionSize, __CxxExceptionFilter, __CxxRegisterExceptionObject, __CxxDetectRethrow, __CxxUnregisterExceptionObject, memmove, __std_exception_copy, _except_handler4_common, memset, __std_type_info_destroy_list, __telemetry_main_return_trigger, __telemetry_main_invoke_trigger, _CxxThrowException, __std_exception_destroy, __FrameUnwindFilter
api-ms-win-crt-runtime-l1-1-0.dll	_cexit, _crt_at_quick_exit, _crt_atexit, _execute_onexit_table, _register_onexit_function, terminate, _initialize_narrow_environment, _seh_filter_dll, _initterm_e, _initterm, _invalid_parameter_noinfo_noreturn, abort, _initialize_onexit_table
api-ms-win-crt-heap-l1-1-0.dll	_callnewh, free, malloc
KERNEL32.dll	IsDebuggerPresent, TerminateProcess, GetCurrentProcess, GetModuleHandleW, IsProcessorFeaturePresent, GetStartupInfoW, SetUnhandledExceptionFilter, UnhandledExceptionFilter, InitializeSListHead, DisableThreadLibraryCalls, GetSystemTimeAsFileTime, GetCurrentThreadId, GetCurrentProcessId, QueryPerformanceCounter, Sleep
MSVCP140.dll	?_Xout_of_range@std@@YAXPBD@Z, ?_Xlength_error@std@@YAXPBD@Z, ?_Xbad_alloc@std@@YAXXZ, ?__ExceptionPtrCopy@@YAXPAXPBX@Z, ?__ExceptionPtrDestroy@@YAXPAX@Z
mscoree.dll	_CorDllMain

Exports

Name	Ordinal	Address
?addZombie@ghostlib@@YAXU_clientData@1@@Z	1	0x100052f5
?deleteZombie@ghostlib@@YAXH@Z	2	0x10004b71
?getZombieCount@ghostlib@@YAHXZ	3	0x10003fbf
?getZombieData@ghostlib@@YAAAU_clientData@1@H@Z	4	0x10003f78
?getZombieIndex@ghostlib@@YAHI@Z	5	0x1000400c
?parseZombie@ghostlib@@YAXIHPAD@Z	6	0x10004030
?updateZombieConnection@ghostlib@@YAXHI@Z	7	0x10003f9a

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/01/21-06:12:11.354122	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/01/21-06:12:11.386419	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
04/01/21-06:12:11.390826	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
04/01/21-06:12:11.423330	ICMP	449	ICMP Time-To-Live Exceeded in Transit			5.56.20.161	192.168.2.6
04/01/21-06:12:11.425257	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
04/01/21-06:12:11.463487	ICMP	449	ICMP Time-To-Live Exceeded in Transit			81.95.15.57	192.168.2.6
04/01/21-06:12:11.464387	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
04/01/21-06:12:11.503349	ICMP	449	ICMP Time-To-Live Exceeded in Transit			152.195.101.202	192.168.2.6
04/01/21-06:12:11.506038	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
04/01/21-06:12:11.544582	ICMP	449	ICMP Time-To-Live Exceeded in Transit			152.195.101.129	192.168.2.6
04/01/21-06:12:11.547408	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
04/01/21-06:12:11.585246	ICMP	408	ICMP Echo Reply			93.184.221.240	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 06:12:04.350193977 CEST	52478	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:04.421039104 CEST	53	52478	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:04.804923058 CEST	58931	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:04.851064920 CEST	53	58931	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:05.289675951 CEST	57725	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:05.367022038 CEST	53	57725	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:07.710818052 CEST	49283	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:07.767781973 CEST	53	49283	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:11.291646004 CEST	58377	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:11.353051901 CEST	53	58377	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:33.010574102 CEST	55074	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:33.059482098 CEST	53	55074	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:33.334621906 CEST	54513	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:33.389134884 CEST	53	54513	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:34.687056065 CEST	62044	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:34.735765934 CEST	53	62044	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:35.593846083 CEST	63791	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:35.651016951 CEST	53	63791	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:36.452940941 CEST	64267	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:36.502856016 CEST	53	64267	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:37.253318071 CEST	49448	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:37.299249887 CEST	53	49448	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:38.299793959 CEST	60342	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:38.348613024 CEST	53	60342	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:39.520942926 CEST	61346	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:39.574888945 CEST	53	61346	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:40.426985979 CEST	51774	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:40.481499910 CEST	53	51774	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:41.281778097 CEST	56023	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:41.336076021 CEST	53	56023	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:42.841733932 CEST	58384	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:42.887624979 CEST	53	58384	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:43.494297028 CEST	60261	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:43.540096045 CEST	53	60261	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:43.682162046 CEST	56061	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:43.730918884 CEST	53	56061	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:44.733933926 CEST	58336	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:44.779882908 CEST	53	58336	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:45.725541115 CEST	53781	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:45.787862062 CEST	53	53781	8.8.8.8	192.168.2.6

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 06:12:52.525274992 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:52.579679966 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:53.006681919 CEST	52811	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:53.062551022 CEST	53	52811	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:58.865503073 CEST	55299	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:58.911446095 CEST	53	55299	8.8.8.8	192.168.2.6
Apr 1, 2021 06:12:59.240751028 CEST	63745	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:12:59.349643946 CEST	53	63745	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:02.900995970 CEST	50055	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:02.948143959 CEST	53	50055	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:16.205322981 CEST	61374	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:16.251156092 CEST	53	61374	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:17.168546915 CEST	50339	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:17.313257933 CEST	53	50339	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:17.979096889 CEST	63307	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:18.043430090 CEST	49694	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:18.052860975 CEST	53	63307	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:18.096448898 CEST	53	49694	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:18.925461054 CEST	54982	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:19.080046892 CEST	53	54982	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:19.436268091 CEST	50010	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:19.490458965 CEST	53	50010	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:19.593916893 CEST	63718	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:19.648113966 CEST	53	63718	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:19.808170080 CEST	62116	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:19.879549980 CEST	53	62116	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:20.314861059 CEST	63816	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:20.369704008 CEST	53	63816	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:20.559622049 CEST	55014	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:20.607620955 CEST	53	55014	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:20.994010925 CEST	62208	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:21.048340082 CEST	53	62208	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:21.588208914 CEST	57574	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:21.634076118 CEST	53	57574	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:21.733527899 CEST	51818	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:21.779480934 CEST	53	51818	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:22.519459009 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:22.584667921 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:23.156303883 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:23.210562944 CEST	53	60778	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:24.425446033 CEST	53799	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:24.474349976 CEST	53	53799	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:25.075439930 CEST	54683	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:25.129590034 CEST	53	54683	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:42.871862888 CEST	59329	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:42.927845955 CEST	53	59329	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:53.295932055 CEST	64021	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:53.351028919 CEST	53	64021	8.8.8.8	192.168.2.6
Apr 1, 2021 06:13:54.324568033 CEST	56129	53	192.168.2.6	8.8.8.8
Apr 1, 2021 06:13:54.378905058 CEST	53	56129	8.8.8.8	192.168.2.6

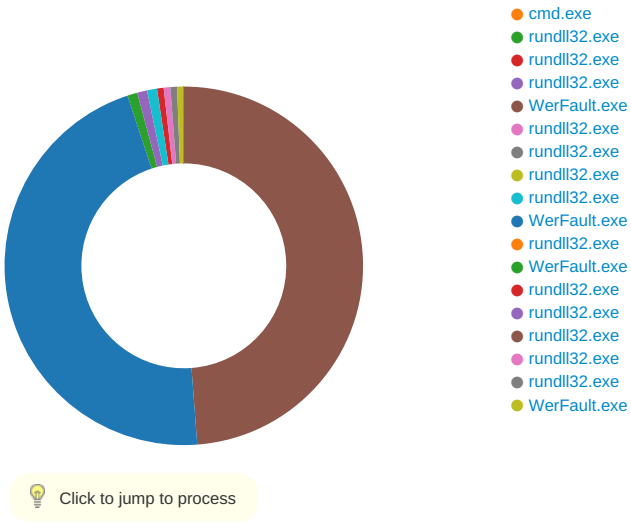
Code Manipulations

Statistics

Behavior

● loaddll32.exe

Copyright Joe Security LLC 2021



System Behavior

Analysis Process: loaddll32.exe PID: 6984 Parent PID: 5248

General

Start time:	06:12:13
Start date:	01/04/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\ghost.dll'
Imagebase:	0x1260000
File size:	122368 bytes
MD5 hash:	0A44868D26BC4DA6847ED7EF6AAFD427
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: 6992 Parent PID: 6984

General

Start time:	06:12:13
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\ghost.dll',#1
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright Joe Security LLC 2021

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 7000 Parent PID: 6984

General

Start time:	06:12:13
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\ghost.dll,?addZombie@ghostlib@@YAXU_clientData@1@@Z
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\rundll32.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E08C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\rundll32.exe.log	unknown	42	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a	1,"fusion","GAC",0..1,"WinRT","NotApp",1..	success or wait	1	6E08C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile

Analysis Process: rundll32.exe PID: 7012 Parent PID: 6992

General

Start time:	06:12:13
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\ghost.dll',#1

Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile

Analysis Process: rundll32.exe PID: 7112 Parent PID: 6984

General

Start time:	06:12:17
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\ghost.dll,?deleteZombie@ghostlib@@YAXH@Z
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile
C:\Users\user\Desktop\ghost.dll	unknown	4096	success or wait	1	6DD3D72F	unknown
C:\Users\user\Desktop\ghost.dll	unknown	512	success or wait	1	6DD3D72F	unknown

Analysis Process: WerFault.exe PID: 6424 Parent PID: 7112

General

Start time:	06:12:19
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7112 -s 1028
Imagebase:	0xb30000

File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7EC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7EC.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_e8ec31b4b32c25a646f8b3a58a24f343d9e92b6_82810a17_1940d40d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_e8ec31b4b32c25a646f8b3a58a24f343d9e92b6_82810a17_1940d40d\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C35497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7EC.tmp	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	success or wait	1	6C354BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	success or wait	1	6C354BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7EC.tmp.xml	success or wait	1	6C354BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7F9.tmp.csv	success or wait	1	6C354BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBCDC.tmp.txt	success or wait	1	6C354BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 b9 c6 65 60 a4 05 12 00 00 00 00 00	MDMP..... .....e`.....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.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 b8 21 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 c8 1b 00 00 b1 c6 65 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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... ....e`.................. ....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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.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 80 34 30 00 8c 34 30 00 ec af 68 73 80 34 30 00 ec af 68 73 8c 34 30 00 68 fa 14 00 76 24 25 04 23 00 00 00 02 02 01 00 54 fa 14 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...+. ..+....40..40...hs.40...hs.40. h...v$%.#.......T...+.........	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	unknown	168	cc 1b 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 76 24 25 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8c 34 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 0a 28 00 00	........................v$%... ....40......... ....(..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	unknown	20	02 01 00 00 e8 32 0a 04 00 00 00 00 54 00 00 00 f6 48 00 00	.....2......T....H..	success or wait	258	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	unknown	84	00 00 00 00 00 00 00 00 e0 91 f3 03 2c 2d e9 ff 9c 53 e9 ff 00 00 00 00 00 00 00 00 00 00 00 00 24 61 04 00 12 00 28 0c 00 00 00 00 79 02 00 00 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00	............,-...S..............$a.... (.....y...v...........	success or wait	257	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	unknown	4	ac 3a 0b 00	.:..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	unknown	4	05 00 00 00	....	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 aa aa aa aa ec af 68 73 00 00 00 00 e8 eb 14 00 bc 9a e5 77 23 00 00 00 02 02 00 00 58 ea 14 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...+. ..+.....................hs.... ....w#.......X...+.........	success or wait	5	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	unknown	48	e8 1b 00 00 01 00 00 00 20 00 00 00 02 00 00 00 00 00 60 29 00 00 00 00 00 48 fa 22 04 00 00 00 00 b8 05 00 00 fa 8e 01 00 cc 02 00 00 06 36 00 00	....`).....H."... .....6..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	unknown	4	37 00 00 00	7...	success or wait	55	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.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	55	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	unknown	752	00 00 5e 6c 00 00 00 00 00 80 0e 00 00 08 0f 00 d5 60 8e 5a e4 27 00 00 bd 04 ef fe 00 00 01 00 07 00 0e 00 00 00 f0 0b 07 00 0e 00 00 00 f0 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 29 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 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 90 9c 02 00 00 00 00 00 30 c9 02 00 00 00 00 b3 42 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 c3 62 03 00 00 00 00 00 c8 67 03 00 00 00 00 00 00 00 00 00 00 00 00 00 33 f7 1a 00 00 00 00 00 0d 08 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 0d 08 05 00 00 00 00	..^l.....`.Z.'..... .....?..... .....)..... ..@A.....Zb..... ....0..... .B.....b.....g .....3..... @.....	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	unknown	15996	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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA77E.tmp.dmp	unknown	108	03 00 00 00 f4 00 00 00 fc 06 00 00 04 00 00 00 38 17 00 00 fc 07 00 00 05 00 00 00 24 10 00 00 d2 38 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 88 28 00 00 25 c2 01 00 15 00 00 00 ec 01 00 00 34 1f 00 00 16 00 00 00 98 00 00 00 20 21 00 00	.....8.....$.....8.....T.....8.....T.....(..%.....4..... !..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.1.1.2.<./.P.i.d.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 34 00 30 00 34 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.>.8.4.0.4.<./.U.p.t.i.m.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 39 00 38 00 31 00 31 00 35 00 33 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.9.8.1.1.5.3.2.8.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 39 00 38 00 31 00 30 00 37 00 31 00 33 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.>.1.9.8.1.0.7.1.3.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 34 00 39 00 37 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.9.7.5.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 37 00 35 00 31 00 34 00 34 00 39 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.>.1.7.5.1.4.4.9.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 37 00 35 00 31 00 34 00 34 00 39 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.>.1.7.5.1.4.4.9.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 35 00 37 00 34 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.5.7.4.3.2.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 35 00 37 00 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.5.7.2.0.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 34 00 31 00 32 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 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.>.4.1.2.5.6.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 34 00 30 00 39 00 38 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.>.4.0.9.8.4.<./.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 39 00 39 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.0.9.9.3.6.6.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 30 00 30 00 30 00 31 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.1.0.0.1.8.5.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 39 00 39 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.1.0.9.9.3.6.6.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 39 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.9.8.4.<./.P.i.d.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0. <./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 33 00 36 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.1.2.3.6.2. <./.U.p.t.i.m.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 31 00 37 00 31 00 31 00 33 00 30 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.7.1.1.3.0.8.8. <./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 31 00 33 00 30 00 38 00 32 00 36 00 32 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.3.0.8.2.6.2.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 39 00 37 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.9.7.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 31 00 37 00 30 00 33 00 30 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.>.3.1.7.0.3.0.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 30 00 36 00 33 00 38 00 30 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.0.6.3.8.0.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 33 00 32 00 35 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.2.5.3.6.<./.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 32 00 34 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.4.6.6.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 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 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.>.5.2.2.4.<./.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.1.3.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.0.2.1.1.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 30 00 33 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.1.0.3.0.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.6.0.2.1.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 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.>.C.L.R.2.0.r.3.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 78 00 6a 00 78 00 6a 00 63 00 66 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.>.x.j.x.j.c.f.,. .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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 78 00 6a 00 78 00 6a 00 63 00 66 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.>.x.j.x.j.c.f.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 34 00 30 00 31 00 35 00 37 00 37 00 36 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.>.1.5.7.4.0.1.5.7.7.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 34 00 2d 00 30 00 31 00 54 00 31 00 33 00 3a 00 31 00 32 00 3a 00 32 00 35 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.4.-.0.1.T.1.3.:.1.2.:.2.5.Z.".>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 31 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 36 00 30 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 36 00 30 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.6.1.". .P.I.D.=.".7.1.1.2.". .U.p.t.i.m.e.M.S.=.".6.0.9.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".6.0.9.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 39 00 66 00 35 00 36 00 61 00 37 00 63 00 2d 00 31 00 64 00 64 00 33 00 2d 00 34 00 36 00 35 00 35 00 2d 00 38 00 64 00 38 00 61 00 2d 00 30 00 30 00 30 00 62 00 65 00 30 00 32 00 34 00 66 00 62 00 61 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.c.9.f.5.6.a.7.c.-.1.d.d.3.-.4.6.5.5.-.8.d.8.a.-.0.0.0.b.e.0.2.4.f.b.a.e.<./.G.u.i.d.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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 34 00 2d 00 30 00 31 00 54 00 31 00 33 00 3a 00 31 00 32 00 3a 00 32 00 35 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.4.-.0.1.T.1.3.:.1.2.:.2.5.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB2AB.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	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7EC.tmp.xml	unknown	4752	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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_e8ec31b4b32c25a646f8b3a58a24f343d9e92b6_82810a17_1940d40d\Report.wer	unknown	2	ff fe	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_e8ec31b4b32c25a646f8b3a58a24f343d9e92b6_82810a17_1940d40d\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	188	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_e8ec31b4b32c25a646f8b3a58a24f343d9e92b6_82810a17_1940d40d\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 32 00 35 00 39 00 39 00 35 00 33 00 30 00 31 00 32 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.2.5.9.9.5.3.0.1.2.	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6C3736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6C371FB2	RegCreateKeyExW
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C3543D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6C3736BF	unknown

Copyright Joe Security LLC 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6C3736BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 76 24 25 04 02 00 00 00 00 00 00 00 8C 34 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6C371FE8	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6384 Parent PID: 6984

General

Start time:	06:12:20
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\ghost.dll,?getZombieCount@ghostlib@@YAHXZ
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Copyright Joe Security LLC 2021

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile

Analysis Process: rundll32.exe PID: 5236 Parent PID: 6984

General

Start time:	06:12:23
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\ghost.dll,?getZombieData@ghostlib@@YAAAU_clientData@1@H@Z
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile

Analysis Process: rundll32.exe PID: 6008 Parent PID: 6984

General

Start time:	06:12:27
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\ghost.dll,?getZombieIndex@ghostlib@@YAHI@Z
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile

Analysis Process: rundll32.exe PID: 6664 Parent PID: 6984

General

Start time:	06:12:31
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\ghost.dll,?parseZombie@ghostlib@@YAXIHPAD@Z
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile
C:\Users\user\Desktop\ghost.dll	unknown	4096	success or wait	1	6DD3D72F	unknown
C:\Users\user\Desktop\ghost.dll	unknown	512	success or wait	1	6DD3D72F	unknown

Analysis Process: WerFault.exe PID: 6728 Parent PID: 6664

General

Start time:	06:12:32
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6664 -s 1028
Imagebase:	0xb30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

Copyright Joe Security LLC 2021

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	6C361717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBFC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBFC.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_facd47adbece4b362bc62fffc58409335218397_82810a17_1a111f1f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_facd47adbece4b362bc62fffc58409335218397_82810a17_1a111f1f\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C35497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBFC.tmp	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	success or wait	1	6C354BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	success or wait	1	6C354BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBFC.tmp.xml	success or wait	1	6C354BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREC2B.tmp.csv	success or wait	1	6C354BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF236.tmp.txt	success or wait	1	6C354BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 c6 c6 65 60 a4 05 12 00 00 00 00 00	MDMP..... .....e`.....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.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 e8 21 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 08 1a 00 00 bf c6 65 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 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... ....e`.................. ....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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 30 40 64 73 a4 fd dc 02 00 00 00 00 4a 36 38 03 00 00 a1 01 9c fd dc 02 0f 24 f3 04 23 00 00 00 46 02 01 00 74 fd dc 02 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.......0@ds........J68..... .....$..#...F...t...+.........	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	unknown	168	f4 19 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 0f 24 f3 04 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 08 00 84 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 3a 28 00 00	........................$.... ....:(..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	unknown	20	05 01 00 00 08 f5 f0 04 00 00 00 00 f8 0a 00 00 22 4c 00 00	..............."L..	success or wait	261	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	unknown	2808	2c 95 e5 77 19 07 ba 76 64 03 00 00 00 00 00 00 50 f5 f0 04 aa aa aa aa 64 03 00 00 aa aa aa aa d8 34 3b 03 24 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 50 f5 f0 04 00 00 00 00 64 03 00 00 74 f5 f0 04 aa aa aa aa a0 f5 f0 04 c0 1e bc 76 aa aa aa aa 00 00 00 00 ac f5 f0 04 ea 3b c0 6d 64 03 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa 00 00 00 00 d0 64 38 03 d8 34 3b 03 ec f5 f0 04 e0 32 15 6e 00 00 00 00 fc f5 f0 04 31 3c c0 6d 00 00 00 00 aa aa aa aa 00 00 00 00 d0 64 38 03 d8 34 3b 03 00 00 00 00 64 03 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 b8 f5 f0 04 e0 f5 f0 04 28 f6 f0 04 b0 1a d3 6d aa aa aa aa 00 00 00 00 34 f6 f0 04 b6 3b c0 6d 00 00 00	,..w...vd.......P.......d..... ...4;.$....................... ....P.......d. ..t..............v............ .;.md....................d8..4 ;......2.n........1<.m........ .....d8..4;.....d............. ....(......m.... ....4....;.m...	success or wait	260	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	unknown	4	ac 3a 0b 00	.:..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	unknown	4	06 00 00 00	....	success or wait	6	6C35497A	unknown

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 08 ef dc 02 bc 9a e5 77 23 00 00 00 06 02 00 00 78 ed dc 02 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+.......................... ....w#.......x...+.........	success or wait	6	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	unknown	48	a0 1b 00 00 01 00 00 00 20 00 00 00 02 00 00 00 00 50 e3 02 00 00 00 00 08 f5 f0 04 00 00 00 00 f8 0a 00 00 22 4c 00 00 cc 02 00 00 02 39 00 00	....P............ ......"L.......9..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	unknown	4	37 00 00 00	7...	success or wait	55	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.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	55	6C35497A	unknown

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	unknown	752	00 00 5e 6c 00 00 00 00 00 00 80 0e 00 00 08 0f 00 d5 60 8e 5a 14 28 00 00 bd 04 ef fe 00 00 01 00 07 00 0e 00 00 00 00 f0 0b 07 00 0e 00 00 00 f0 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 e0 8c 02 00 00 00 00 00 30 c9 02 00 00 00 00 48 4c 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 96 70 03 00 00 00 00 00 ff 70 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d1 e7 1a 00 00 00 00 00 6f 17 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 db 31 05 00 00 00 00	..^l.....`.Z.(..... .....?..... .....)..... ..@A.....Zb..... ....0..... HL.....p.....p .....o..... @.....1.....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	unknown	15996	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	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD778.tmp.dmp	unknown	108	03 00 00 00 24 01 00 00 fc 06 00 00 04 00 00 00 38 17 00 00 2c 08 00 00 05 00 00 00 54 10 00 00 ce 3b 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 88 28 00 00 6a e1 01 00 15 00 00 00 ec 01 00 00 64 1f 00 00 16 00 00 00 98 00 00 00 50 21 00 00	....$.....8...,.....T. ...;.....T.....8..... ....T.....(..j..... ..d.....P!..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 36 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.6.6.4.<./.P.i.d.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 38 00 30 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.7.8.0.8.<./.U.p.t.i.m.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 39 00 37 00 35 00 39 00 31 00 30 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.>.1.9.7.5.9.1.0.4.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 39 00 37 00 35 00 38 00 32 00 38 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.>.1.9.7.5.8.2.8.4.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 34 00 39 00 35 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.>.4.9.5.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 37 00 34 00 32 00 38 00 34 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.7.4.2.8.4.8.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 37 00 34 00 32 00 38 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.7.4.2.8.4.8.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 35 00 37 00 34 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.5.7.4.3.2.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 35 00 37 00 34 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.5.7.4.3.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 34 00 31 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.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.>.4.1.1.3.6.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 34 00 30 00 38 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.>.4.0.8.6.4.<./.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 30 00 33 00 30 00 35 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.1.0.3.0.5.2.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 30 00 34 00 32 00 38 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.1.0.4.2.8.1.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 30 00 33 00 30 00 35 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.1.1.0.3.0.5.2.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 39 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.9.8.4.<./.P.i.d.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 35 00 35 00 33 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.5.5.3.4.<./.U.p.t.i.m.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 30 00 34 00 32 00 34 00 31 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.>.6.0.4.2.4.1.9.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 33 00 32 00 32 00 33 00 34 00 32 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.3.2.2.3.4.2.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 39 00 34 00 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.>.1.9.4.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 32 00 32 00 31 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.>.6.2.2.1.8.2.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 31 00 31 00 35 00 33 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.>.6.1.1.5.3.2.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.1.5.1.8.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 30 00 39 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.0.9.9.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 39 00 35 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.5.7.6.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 31 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.1.2.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 33 00 35 00 31 00 36 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.>.1.3.5.1.6.8.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 33 00 35 00 39 00 38 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.>.1.3.5.9.8.7.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 33 00 35 00 31 00 36 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.>.1.3.5.1.6.8.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 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.>.C.L.R.2.0.r.3.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 78 00 6a 00 78 00 6a 00 63 00 66 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.>.x.j.x.j.c.f.,. .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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 78 00 6a 00 78 00 6a 00 63 00 66 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.>.x.j.x.j.c.f.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 34 00 30 00 31 00 35 00 37 00 37 00 36 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.>.1.5.7.4.0.1.5.7.7.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 34 00 2d 00 30 00 31 00 54 00 31 00 33 00 3a 00 31 00 32 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.-.0.4.-.0.1.T.1.3.:.1.2.:.3.9.Z.".>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 37 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 36 00 36 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 37 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 37 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 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.7.2.". .P.I.D.=.".6.6.6.4.". .U.p.t.i.m.e.M.S.=.".7.3.4.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".7.3.4.". .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.=.".1."	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 30 00 34 00 62 00 31 00 34 00 61 00 35 00 2d 00 31 00 32 00 39 00 34 00 2d 00 34 00 63 00 36 00 61 00 2d 00 62 00 66 00 36 00 35 00 2d 00 32 00 35 00 35 00 32 00 31 00 66 00 66 00 30 00 63 00 62 00 38 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.f.0.4.b.1.4.a.5.-.1.2.9.4.-.4.c.6.a.-.b.f.6.5.-.2.5.5.2.1.f.f.0.c.b.8.3.<./.G.u.i.d.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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 34 00 2d 00 30 00 31 00 54 00 31 00 33 00 3a 00 31 00 32 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.-.0.4.-.0.1.T.1.3.:.1.2.:.3.9.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE61F.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	6C35497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBFC.tmp.xml	unknown	4750	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	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_facd47adbece4b362bc62fffc58409335218397_82810a17_1a111f1f\Report.wer	unknown	2	ff fe	..	success or wait	1	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_facd47adbece4b362bc62fffc58409335218397_82810a17_1a111f1f\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	188	6C35497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_facd47adbece4b362bc62fffc58409335218397_82810a17_1a111f1f\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 32 00 33 00 31 00 34 00 30 00 35 00 38 00 32 00 30 00	M.e.t.a.d.a.t.a.H.a.s.h.=.2.3.1.4.0.5.8.2.0.	success or wait	1	6C35497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C3736BF	unknown
\REGISTRY\A\{ba6641e4-c27a-5790-a11a-d1a22aac2af1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C3543D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

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

Copyright Joe Security LLC 2021

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 76 24 25 04 02 00 00 00 00 00 00 00 8C 34 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 0F 24 F3 04 02 00 00 00 01 00 00 00 08 00 84 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C371FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: 6828 Parent PID: 6984

General

Start time:	06:12:34
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\ghost.dll,?updateZombieConnection@ghostlib@@YAXHI@Z
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: WerFault.exe PID: 6900 Parent PID: 6828

General

Start time:	06:12:36
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6828 -s 1028
Imagebase:	0xb30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: rundll32.exe PID: 6696 Parent PID: 6984

General

Start time:	06:12:37
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\ghost.dll',?addZombie@ghostlib@@YAXU_clientData@1@@Z
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true

Copyright Joe Security LLC 2021

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: rundll32.exe PID: 7056 Parent PID: 6984

General

Start time:	06:12:38
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\ghost.dll',?deleteZombie@ghostlib@@YAXH@Z
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: rundll32.exe PID: 1724 Parent PID: 6984

General

Start time:	06:12:38
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\ghost.dll',?getZombieCount@ghostlib@@YAHXZ
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: rundll32.exe PID: 6152 Parent PID: 6984

General

Start time:	06:12:38
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\ghost.dll',?getZombieData@ghostlib@@YAAAU_clientData@1@H@Z
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: rundll32.exe PID: 1864 Parent PID: 6984

General

Start time:	06:12:39
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\ghost.dll',?getZombieIndex@ghostlib@@YAHI@Z
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: WerFault.exe PID: 6360 Parent PID: 7056

General

Start time:	06:12:40
Start date:	01/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7056 -s 1028
Imagebase:	0xb30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis

Copyright Joe Security LLC 2021