ID: 625078
Sample Name: EXPORT INVOICE.pdf.scr
Cookbook: default.jbs
Time: 11:48:04
Date: 12/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

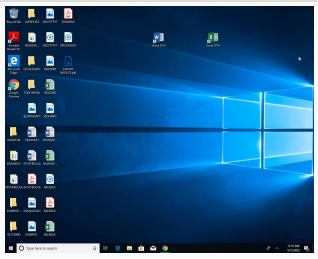
Windows Analysis Report

EXPORT INVOICE.pdf.scr

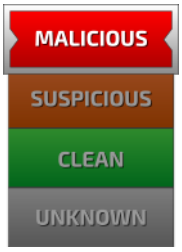
Overview

General Information

Sample Name:	EXPORT INVOICE.pdf.scr (renamed file extension from scr to exe)
Analysis ID:	625078
MD5:	2cf09341b87d20..
SHA1:	ec9de894d7cb09..
SHA256:	2b21885c68cf8b…
Tags:	exe
Infos:	



Detection

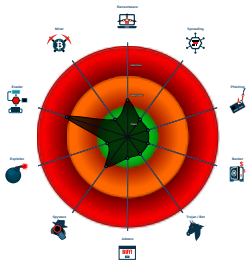


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Initial sample is a PE file and has a…
- Uses an obfuscated file name to hid…
- Machine Learning detection for sam…
- Uses 32bit PE files
- Queries the volume information (nam…
- Sample file is different than original …
- One or more processes crash
- PE file contains strange resources
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- EXPORT INVOICE.pdf.exe (PID: 7108 cmdline: "C:\Users\user\Desktop\EXPORT INVOICE.pdf.exe" MD5: 2CF09341B87D20404A6D824305EA5419)
  - WerFault.exe (PID: 5336 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7108 -s 1280 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

Initial sample is a PE file and has a suspicious name

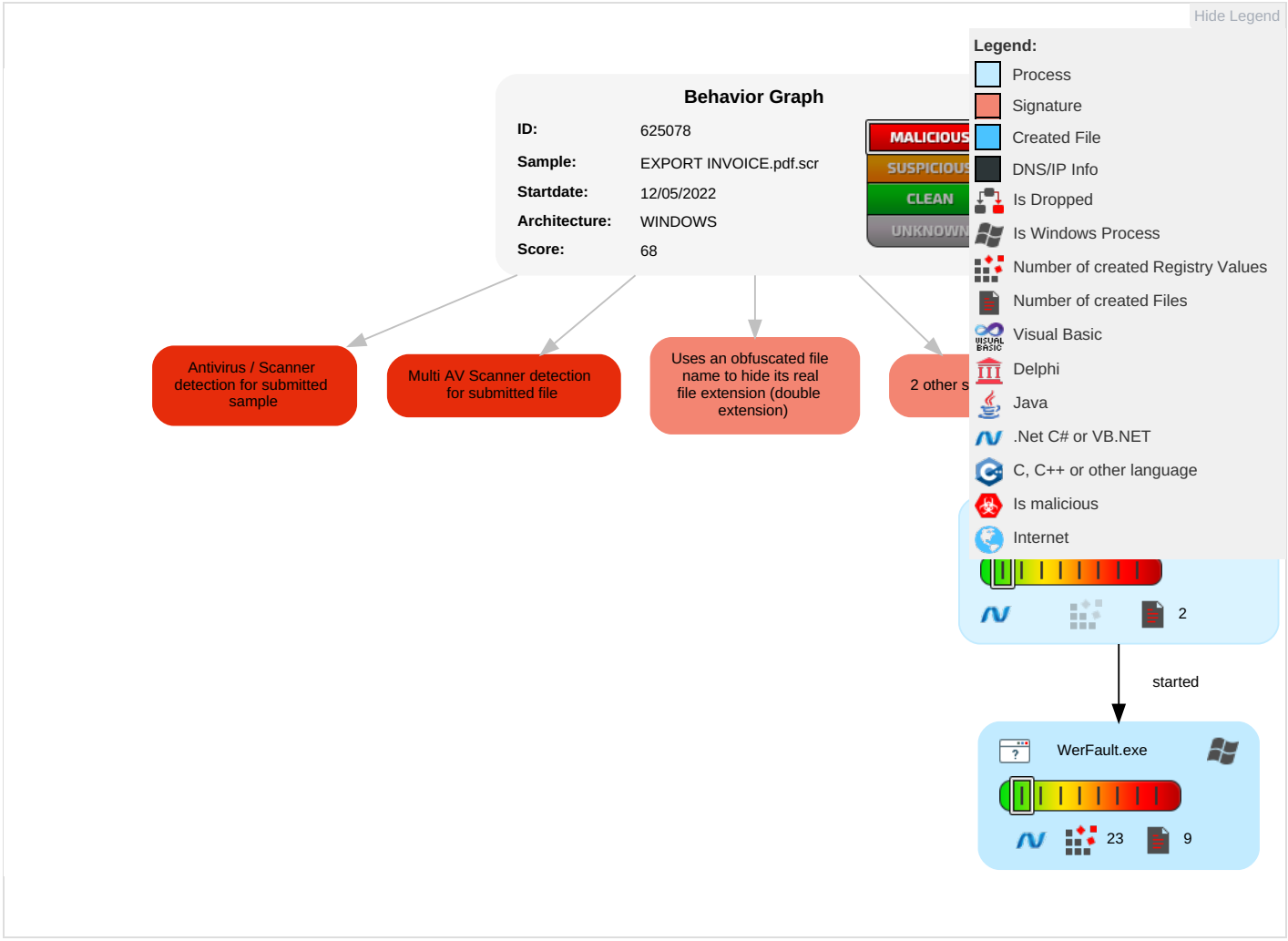
Hooking and other Techniques for Hiding and Protection

Uses an obfuscated file name to hide its real file extension (double extension)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	1 2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Software Packing	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Process Injection	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 2 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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
EXPORT INVOICE.pdf.exe	37%	Virustotal		Browse
EXPORT INVOICE.pdf.exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
EXPORT INVOICE.pdf.exe	100%	Avira	HEUR/AGEN.1202539	
EXPORT INVOICE.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.EXPORT INVOICE.pdf.exe.ef0000.0.unpack	100%	Avira	HEUR/AGEN.1244320		Download File
1.0.EXPORT INVOICE.pdf.exe.ef0000.0.unpack	100%	Avira	HEUR/AGEN.1244320		Download File
1.0.EXPORT INVOICE.pdf.exe.ef0000.1.unpack	100%	Avira	HEUR/AGEN.1244320		Download File

Source	Detection	Scanner	Label	Link	Download
1.0.EXPORT INVOICE.pdf.exe.ef0000.4.unpack	100%	Avira	HEUR/AGEN.1244320		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cndnl	0%	Avira URL Cloud	safe	
http://en.wM	0%	Avira URL Cloud	safe	
http://www.sakkal.comrmW	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fonts.comW	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cnD	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fonts.comWT	0%	Avira URL Cloud	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://www.fontbureau.comionm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.typography.netr	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fonts.com;	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cndnl	EXPORT INVOICE.pdf.exe, 00000001.00000003.376953483.0000000008647000.00000004.00000800.00020000.00000000.sdmp, EXPORT INVOICE.pdf.exe, 00000001.00000003.377031607.0000000008648000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false		high
http://en.wM	EXPORT INVOICE.pdf.exe, 00000001.00000003.370373493.000000000867D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.comrmW	EXPORT INVOICE.pdf.exe, 00000001.00000003.379986920.000000000864D000.00000004.00000800.00020000.00000000.sdmp, EXPORT INVOICE.pdf.exe, 00000001.00000003.379854422.000000000864E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	EXPORT INVOICE.pdf.exe, 00000001.00000000.415970243.0000000008640000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comW	EXPORT INVOICE.pdf.exe, 00000001.00000003.371043084.000000000867D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnD	EXPORT INVOICE.pdf.exe, 00000001.00000003.376953483.0000000008647000.00000004.00000800.00020000.00000000.sdmp, EXPORT INVOICE.pdf.exe, 00000001.00000003.377031607.0000000008648000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	EXPORT INVOICE.pdf.exe, 00000001.00000003.376953483.0000000008647000.00000004.00000800.00020000.00000000.sdmp, EXPORT INVOICE.pdf.exe, 00000001.00000003.377031607.0000000008648000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	EXPORT INVOICE.pdf.exe, 00000001.00000000.412177175.0000000009852000.00000004.00000800.00020000.00000000.sdmp, EXPORT INVOICE.pdf.exe, 00000001.00000003.376953483.0000000008647000.00000004.00000800.00020000.00000000.sdmp, EXPORT INVOICE.pdf.exe, 00000001.00000003.377031607.0000000008648000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	EXPORT INVOICE.pdf.exe, 00000001.0000000 0.412177175.0000000009852000.00000004.00 000800.00020000.00000000.sdmp	false		high
http://www.fonts.comWT	EXPORT INVOICE.pdf.exe, 00000001.0000000 3.371122582.000000000867D000.00000004.00 000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.net	EXPORT INVOICE.pdf.exe, 00000001.0000000 3.371908716.0000000008647000.00000004.00 000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comionm	EXPORT INVOICE.pdf.exe, 00000001.0000000 0.415970243.0000000008640000.00000004.00 000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	EXPORT INVOICE.pdf.exe, 00000001.0000000 0.412177175.0000000009852000.00000004.00 000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como	EXPORT INVOICE.pdf.exe, 00000001.0000000 0.415970243.0000000008640000.00000004.00 000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	EXPORT INVOICE.pdf.exe, 00000001.0000000 0.412177175.0000000009852000.00000004.00 000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	EXPORT INVOICE.pdf.exe, 00000001.0000000 0.412177175.0000000009852000.00000004.00 000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	EXPORT INVOICE.pdf.exe, 00000001.0000000 3.371092907.000000000867D000.00000004.00 000800.00020000.00000000.sdmp, EXPORT IN VOICE.pdf.exe, 00000001.00000000.4121771 75.0000000009852000.00000004.00000800.00 020000.00000000.sdmp, EXPORT INVOICE.pdf.exe, 00000001.00000003.371122582.000000000867D000 .00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	EXPORT INVOICE.pdf.exe, 00000001.0000000 0.412177175.0000000009852000.00000004.00 000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netr	EXPORT INVOICE.pdf.exe, 00000001.0000000 3.373268434.0000000008648000.00000004.00 000800.00020000.00000000.sdmp, EXPORT IN VOICE.pdf.exe, 00000001.00000003.3732297 68.0000000008647000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	EXPORT INVOICE.pdf.exe, 00000001.0000000 0.412177175.0000000009852000.00000004.00 000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	EXPORT INVOICE.pdf.exe, 00000001.0000000 0.412177175.0000000009852000.00000004.00 000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	EXPORT INVOICE.pdf.exe, 00000001.0000000 0.412177175.0000000009852000.00000004.00 000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com;	EXPORT INVOICE.pdf.exe, 00000001.0000000 3.371092907.000000000867D000.00000004.00 000800.00020000.00000000.sdmp, EXPORT IN VOICE.pdf.exe, 00000001.00000003.3710430 84.000000000867D000.00000004.00000800.00 020000.00000000.sdmp, EXPORT INVOICE.pdf.exe, 00000001.00000003.371122582.000000000867D000 .00000004.00000800.00020000.00000000.sdmp, EXPORT INVOICE.pdf.exe, 00000001.0000 0003.371160843.000000000867D000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	625078
Start date and time: 12/05/202211:48:04	2022-05-12 11:48:04 +02:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 6m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	EXPORT INVOICE.pdf.scr (renamed file extension from scr to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.evad.winEXE@2/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 2.8% (good quality ratio 1.5%) • Quality average: 33.8% • Quality standard deviation: 38.3%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.20
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, onedsblobprdwus15.westus.cloudapp.azure.com, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:49:32	API Interceptor	1x Sleep call for process: EXPORT INVOICE.pdf.exe modified
11:49:44	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_EXPORT INVOICE.p_b5f6764852466b593dfad674787e99291849f4a4_5c0e5d72_148dd68c\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.1180961660191344
Encrypted:	false
SSDEEP:	192:8So+ZrokHBUZMXyaKeCikHKvi/u7s+S274ltV3N:NoGssBUZMXyaO/u7s+X4ltV3N
MD5:	1F31080612E3F6C4532346FCD3D5C016
SHA1:	E42CCD16F84BFF420021EB2BA9DDC537F737FEFC
SHA-256:	0B7453D7AA239FECF7864F1B5810B4F239D115F609136131996FADE243151C30
SHA-512:	A3F6052AD7416A4CEE823CE102D4B70A0CD2776752D9E80DA14F36AAF8403B64BB478A0DA196CF549EA84BD4604F858D75D6F0EEA2FAA9E48C6E64E2E74BF263
Malicious:	false
Reputation:	low
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.=.1.3.2.9.6.8.5.4.9.8.0.1.9.8.2.6.8.4.....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.=.1.3.2.9.6.8.5.4.9.8.3.5.4.2.0.2.8.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.4.1.1.6.5.9.5.-.5.a.5.9.-.4.3.a.0.-.9.d.c.7.-.4.7.c.7.9.e.6.5.0.9.1.a.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.9.c.a.f.e.2.9.-.b.d.f.a.-.4.b.6.4.-.9.3.1.d.-.8.9.9.1.a.8.1.5.5.e.b.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.E.X.P.O.R.T. .I.N.V.O.I.C.E...p.d.f...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.I.R.u.n.t.i.m.e.E.v.i.d.e.n.c.e.F.a.c.t...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.c.4.-.0.0.0.1.-.0.0.1.8.-.3.b.2.f.-.d.e.f.8.3.0.6.6.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.c.c.3.a.0.5.7.5.0.3.1.8.a.8.8.8.9.c.8.8.1.7.4.f.9.f.2.7.b.8.2.9.0.0.0.0.0.0.0.0.!.0.0.0.0.e.c.9.d.e.8.9.4.d.7.c.b.0.9.e.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 12 18:49:40 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	259748
Entropy (8bit):	4.124164669491366
Encrypted:	false
SSDEEP:	3072:nO1ljd+p2SN0o9gIOgF5xc0+TUCgUDHoPtk+Dl0dopIXuq2:O16pV0o9RpDqHTjrmtrR0dX
MD5:	27132ED0DF055D722D2EC7D30A3BDDD1
SHA1:	E1849483F307B97C1BE9B2A6DACAFDE31DDE71CD
SHA-256:	BFC754BC356FF8C2723F75F675A88A0409EC663F30208D4C484859717C3A8C94
SHA-512:	D89C84400ADEE3F24E833CE23C7A8DADA0D8242E0E40457AEE0C3979B604121CA73CD5F2D0E1240840EE5A24AB8D5D7EFEB03B224B603CB0A0D376A1313CCA83
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....V}b.....'...F.....T.....8.....T.....1..... ....."....U.....B.....P#.....GenuineIntelW.....T.....V}b.....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.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.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):	8452
Entropy (8bit):	3.7133404895699718
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiO56B6YfgSUpvy3MgmfZDYSoCpr989bP0sfOFm:RrlsNiY6B6YoSUpvycgmfNYSKPnfd
MD5:	468747CA40B4B83F9FBB334CD4B3A34D
SHA1:	E53798256597E7463D2E62655E6935F4EC4F12D0
SHA-256:	B73923FC0A208D55F89E62E3FB86058EB8C90884C3EF86A17B13A59FBE0A833C
SHA-512:	EF1C78E9AEE301304FF0E16F83D4055322D1E0855DBE0CB9FC4CD027039F5F251ED4B1B0D437E866D10FCABA644CF7300FDD384E11E6702EEABCEEAA20649 7D
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.0. 8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBA1.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4805
Entropy (8bit):	4.563561801184721
Encrypted:	false
SSDEEP:	48:cvIwSD8zsTJgtWI9ILyWgc8sqYjw18fm8M4JgB8zL8Fd+q8vozLMPn0ulZpAdOIk:uITftr3grsqYMCJghKnXlrAQIOd
MD5:	F4BFB7BF17BB4D09E417682C912EE9AC
SHA1:	4DF54B023773CB7754A7D510F1A2A6E87A0C7B19
SHA-256:	FBA7016993C3260F687045760192ED38E4B5997D982685365C70CD12B8779250
SHA-512:	B4563B3E695B5CFDDFF7014ADB27861463172DFD0CA5E264C350065F04AC8AFCFA3562E0ACCA7429DFE3377F04C5F349AE1D52BBF7460E928D88E4932A21CF CE
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" /> .. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1512240" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0- 11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.125237039189151
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	EXPORT INVOICE.pdf.exe
File size:	808448
MD5:	2cf09341b87d20404a6d824305ea5419
SHA1:	ec9de894d7cb09ed3940db31dfc7a39cc1280acd
SHA256:	2b21885c68cf8bcee3be7e08574372130a42c74a047b1f962cc5e270bb7b543e
SHA512:	db8e247a8192ee53b96ee12a9b1e120e904b58b96f5ea3687d10bda3ea16d479bfe2da0db07b633b35bc03da9665d8ebe13a0e494a481bd88a76c30b79c2dbe9
SSDEEP:	12288:cWRXIfWktOMzKcDOGjBTu2KSgaLfqGC7vh9KBYhLWWZ0u9zfLWt6l/4MKOC6ZEKA:ciXIfWcKwj9wSgajqh7J9K6hLPSu9O
TLSH:	B905BE9872D0B5AECB07C93289545C25A9203C67439AD20B6CC736DFE9BD69ECE041F3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{b.....0..... .....@.. .....@.....

File Icon

	
Icon Hash:	24e4c69696b2d4cc

Static PE Info

General

Entrypoint:	0x4adaee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627BF1C4 [Wed May 11 17:26:28 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
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
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
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xada9c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xae000	0x19578	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xabaf4	0xabc00	False	0.839913402929	data	7.63374734815	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xae000	0x19578	0x19600	False	0.0630484144089	data	1.45882239786	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc8000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xae220	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xae688	0x877	PNG image data, 256 x 256, 8-bit colormap, non-interlaced		
RT_ICON	0xaef00	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xb14a8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xb2550	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xc2d78	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xc6fa0	0x5a	data		
RT_VERSION	0xc6ffc	0x38c	PGP symmetric key encrypted data - Plaintext or unencrypted data		
RT_MANIFEST	0xc7388	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

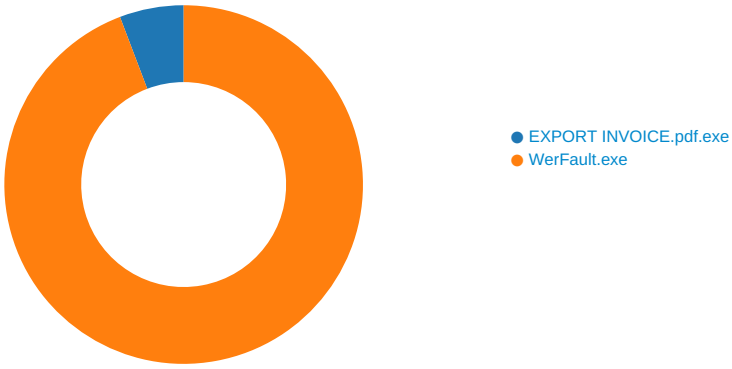
Version Infos	
Description	**Data**
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020 Havy Alegria
Assembly Version	1.0.0.0
InternalName	IRuntimeEvidenceFact.exe
FileVersion	1.0.0.0
CompanyName	Havy Alegria
LegalTrademarks	
Comments	
ProductName	InnoExtractor
ProductVersion	1.0.0.0
FileDescription	InnoExtractor
OriginalFilename	IRuntimeEvidenceFact.exe

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXPORT INVOICE.pdf.exe PID: **7108**, Parent PID: **1984**

General	
Target ID:	1
Start time:	11:49:12
Start date:	12/05/2022
Path:	C:\Users\user\Desktop\EXPORT INVOICE.pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\EXPORT INVOICE.pdf.exe"

Imagebase:	0xef0000
File size:	808448 bytes
MD5 hash:	2CF09341B87D20404A6D824305EA5419
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC6CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC6CF06	unknown

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	6DC45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC45705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBA03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC4CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBA03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BF91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BF91B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DC2D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DC2D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6DC2D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6DC2D72F	unknown
C:\Users\user\Desktop\EXPORT INVOICE.pdf.exe	unknown	4096	success or wait	1	6DC2D72F	unknown
C:\Users\user\Desktop\EXPORT INVOICE.pdf.exe	unknown	512	success or wait	1	6DC2D72F	unknown

Analysis Process: WerFault.exe PID: **5336**, Parent PID: **7108**

General

Target ID:	7
Start time:	11:49:39
Start date:	12/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7108 -s 1280

Imagebase:	0xe20000
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\WERC3FE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBA1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBA1.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_EXPORT INVOICE.p_b5f6764852466b5 93dfad674787e99291849f4a4_5c0e5d72_148dd68c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_EXPORT INVOICE.p_b5f6764852466b5 93dfad674787e99291849f4a4_5c0e 5d72_148dd68c\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7231497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBA1.tmp	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBA1.tmp.xml	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCCC8.tmp.csv	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF1B.tmp.txt	success or wait	1	7231497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 56 7d 62 fd 05 12 00 00 00 00 00	MDMP V}b	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	9040	6	00 00 00 00 00 00		success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 50 23 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 1b 00 00 fd 56 7d 62 00 00 00 00 03 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 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	UBP#GenuineIntelWTV}b 0Pacific Standard TimePacific Daylight Time	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	10790	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 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 01 00 00 00 fd fd 35 01 05 00 00 00 00 00 00 00 05 00 00 00 fd fd 35 01 38 fd 35 01 22 fd fd 73 23 00 00 00 12 02 20 00 fd fd 35 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++5585"s# 5+	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	1620	168	fd 1b 00 00 00 00 00 00 52 43 43 fd 01 00 00 00 00 00 00 00 00 00 00 00 22 fd fd 73 00 00 00 00 05 00 00 00 00 00 00 00 04 16 13 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 6d 00 00 00 00 fd 21 41 01 00 00 00 00 fd fd 35 01 00 00 00 00 01 00 00 00 00 00 00 00 e3 fd 6d 00 00 00 00 fd fd 35 01 00 00 00 00 14 fd 29 03 00 00 00 00 fd fd 3f 01 00 00 00 00 fd fd 35 01 00 00 00 00 5c fd 35 01 00 00 00 00 00 fd 35 01 00 00 00 00 fd 02 00 00 26 2a 00 00	RCC"sm!A5m5)?5\55&*	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	17950	20	71 02 00 00 00 00 fd 6b 00 00 00 00 40 00 00 00 32 6d 00 00	qk@2m	success or wait	625	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	27954	64	4d 5a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00	MZ@	success or wait	624	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	235608	4096	3c fd 3c 05 00 00 3d 05 00 fd 3c 05 00 00 00 00 00 1e 00 00 00 00 00 00 00 50 02 01 00 00 00 00 fd 1b 00 00 fd 14 00 00 00 00 00 00 00 fd 43 01 00 60 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 1a 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	<<=<PC`pw	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	1788	4	09 00 00 00		success or wait	9	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	11506	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 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd 00 00 00 00 fd fd 35 01 fd fd 2f 77 23 00 00 00 02 02 20 00 68 fd 35 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++5/w# h5+	success or wait	9	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	2176	48	34 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 40 03 01 00 00 00 00 14 fd 02 0a 00 00 00 00 fd 03 00 00 29 5f 01 00 fd 02 00 00 52 43 00 00	4 @)_RC	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	2236	4	39 00 00 00	9	success or wait	57	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	9046	50	2c 00 00 00 45 00 58 00 50 00 4f 00 52 00 54 00 20 00 49 00 4e 00 56 00 4f 00 49 00 43 00 45 00 2e 00 70 00 64 00 66 00 2e 00 65 00 78 00 65 00 00 00	,EXPORT INVOICE.pdf.exe	success or wait	57	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	8288	752	00 00 35 6f 00 00 00 00 00 fd 0e 00 00 08 0f 00 fd 60 fd 5a 00 2a 00 00 fd 04 fd fd 00 00 01 00 07 00 0e 00 00 00 fd 0b 07 00 0e 00 00 00 fd 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 00 29 00 00 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 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 30 fd 02 00 00 00 00 39 4e 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 5d fd 03 00 00 00 00 00 37 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 31 fd 1a 00 00 00 00 00 0f 51 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 64 05 00 00 00 00	5o`Z*?)@AZb09N]71Q@d	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	239704	20044	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 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	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3FE.tmp.dmp	32	108	03 00 00 00 fd 01 00 00 fd 06 00 00 04 00 00 00 10 18 00 00 fd 08 00 00 05 00 00 00 14 27 00 00 1e 46 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 31 00 00 0c fd 03 00 15 00 00 00 fd 01 00 00 fd 20 00 00 16 00 00 00 fd 00 00 00 fd 22 00 00	'FT8T1 ''	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	270	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	<Build>17134</Build>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	478	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	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	620	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	<Revision>1</Revision>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	824	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	<LCID>1033</LCID>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7108</Pid>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1002	90	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 45 00 58 00 50 00 4f 00 52 00 54 00 20 00 49 00 4e 00 56 00 4f 00 49 00 43 00 45 00 2e 00 70 00 64 00 66 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>EXPORT INVOICE.pdf.exe</ImageName>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1092	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1096	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1100	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	<CmdLineSignature>000 00000</CmdLineSignature>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1190	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1194	2	09 00		success or wait	2	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1198	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 39 00 31 00 33 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>29134</Uptime>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1242	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1246	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1250	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	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1332	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1336	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1340	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1392	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1396	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1400	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1444	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1448	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1454	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 32 00 39 00 36 00 30 00 36 00 37 00 30 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>296067072</PeakVirtualSize>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1542	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1546	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1552	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 32 00 38 00 39 00 34 00 33 00 39 00 37 00 34 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	<VirtualSize>289439744</VirtualSize>	success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1624	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1628	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1634	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 31 00 31 00 38 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>31183</PageFaultCount>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1710	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1714	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1720	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 35 00 39 00 32 00 37 00 33 00 32 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>59273216</PeakWorkingSetSize>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1818	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1822	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1828	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 35 00 39 00 32 00 37 00 33 00 32 00 31 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>59273216</WorkingSetSize>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1910	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1914	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	1920	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 34 00 32 00 31 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>421448</QuotaPeakPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2034	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2038	2	09 00		success or wait	3	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2044	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 33 00 39 00 38 00 31 00 32 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	<QuotaPagedPoolUsage>398128</QuotaPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2142	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2146	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2152	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 30 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>290440</QuotaPeakNonPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2278	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2282	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2288	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 30 00 30 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>290088</QuotaNonPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2398	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2402	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2408	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 34 00 34 00 31 00 30 00 35 00 37 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>44105728</PagefileUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2486	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2490	2	09 00		success or wait	3	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2496	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 34 00 34 00 36 00 31 00 37 00 37 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>44617728</PeakPagefileUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2590	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2594	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2600	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 34 00 34 00 31 00 30 00 35 00 37 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>44105728</PrivateUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2674	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2678	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2682	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2736	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2766	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2770	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2776	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2816	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2820	2	09 00		success or wait	4	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2828	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3688</Pid>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2858	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2862	2	09 00		success or wait	4	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2870	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2940	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2944	2	09 00		success or wait	4	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	2952	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3042	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3046	2	09 00		success or wait	4	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3054	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 36 00 32 00 30 00 37 00 35 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5620758</Uptime>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3102	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3106	2	09 00		success or wait	4	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3114	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3192	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3196	2	09 00		success or wait	4	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3204	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3256	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3260	2	09 00		success or wait	4	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3268	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3312	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3316	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3326	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3416	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3420	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3430	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3504	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3508	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3518	76	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 33 00 39 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>49391</PageFaultCount>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3594	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3598	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3608	100	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 30 00 33 00 32 00 32 00 37 00 33 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>103227392</PeakWorkingSetSize>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3708	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3712	2	09 00		success or wait	5	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3722	84	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 30 00 32 00 39 00 30 00 37 00 39 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>102907904</WorkingSetSize>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3806	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3810	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3820	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 39 00 37 00 38 00 36 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>978648</QuotaPeakPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3934	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3938	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	3948	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 39 00 34 00 37 00 38 00 34 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	<QuotaPagedPoolUsage>947848</QuotaPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4046	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4050	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4060	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 37 00 34 00 37 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>74776</QuotaPeakNonPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4184	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4188	2	09 00		success or wait	5	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4198	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 37 00 32 00 36 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>72600</QuotaNonPagedPoolUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4306	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4310	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4320	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 33 00 34 00 36 00 38 00 39 00 30 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>34689024</PagefileUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4398	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4402	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4412	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 33 00 36 00 37 00 32 00 38 00 38 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>36728832</PeakPagefileUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4506	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4510	2	09 00		success or wait	5	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4520	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 33 00 34 00 36 00 38 00 39 00 30 00 32 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>34689024</PrivateUsage>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4594	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4598	2	09 00		success or wait	4	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4606	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4652	4	0d 00 0a 00		success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4656	2	09 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4662	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4712	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4744	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4748	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4750	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4792	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4796	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4798	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4836	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4840	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4844	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	<EventType>CLR20r3</EventType>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4904	4	0d 00 0a 00		success or wait	9	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4908	2	09 00		success or wait	18	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	4912	94	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 45 00 58 00 50 00 4f 00 52 00 54 00 20 00 49 00 4e 00 56 00 4f 00 49 00 43 00 45 00 2e 00 70 00 64 00 66 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	<Parameter0>EXPORT INVOICE.pdf .exe</Parameter0>	success or wait	9	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	5628	4	0d 00 0a 00		success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	5632	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	5634	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	5674	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	5678	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	5680	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	5718	4	0d 00 0a 00		success or wait	6	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	5722	2	09 00		success or wait	12	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	5726	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	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6286	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6326	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6330	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6332	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6370	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6374	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6378	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	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6472	4	0d 00 0a 00		success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6476	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6480	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 6a 00 78 00 6e 00 70 00 69 00 6c 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>jxnpil, Inc.</SystemManufacturer>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6586	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6590	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6594	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 6a 00 78 00 6e 00 70 00 69 00 6c 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	<SystemProductName>jxnpil7,1</SystemProductName>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6690	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6694	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6698	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 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6818	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6822	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6826	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 39 00 31 00 31 00 30 00 32 00 38 00 34 00 34 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1591102844</OSInstallDate>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6908	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6912	2	09 00		success or wait	2	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	6916	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	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7018	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7022	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7026	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	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7100	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7140	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7144	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7146	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7188	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7284	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7288	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7290	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7326	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7330	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7332	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7356	4	0d 00 0a 00		success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7360	2	09 00		success or wait	6	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7364	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 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7622	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7626	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7628	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7654	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7658	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7660	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 32 00 2d 00 30 00 35 00 2d 00 31 00 32 00 54 00 31 00 38 00 3a 00 34 00 39 00 3a 00 34 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-12T18:49:41Z">	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7760	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7764	2	09 00		success or wait	2	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	7768	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 30 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 31 00 31 00 35 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 31 00 31 00 35 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<Process AsId="406" PID="7108" UptimeMS="21156" TimeSinceCreationMS="21156" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8034	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8038	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8042	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8062	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8066	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8068	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8106	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8110	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8112	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8158	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 34 00 31 00 31 00 36 00 35 00 39 00 35 00 2d 00 35 00 61 00 35 00 39 00 2d 00 34 00 33 00 61 00 30 00 2d 00 39 00 64 00 63 00 37 00 2d 00 34 00 37 00 63 00 37 00 39 00 65 00 36 00 35 00 30 00 39 00 31 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>64116595-5a59-43a0-9dc7-47c79e65091a</Guid>	success or wait	1	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8256	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8260	2	09 00		success or wait	2	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8264	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 32 00 2d 00 30 00 35 00 2d 00 31 00 32 00 54 00 31 00 38 00 3a 00 34 00 39 00 3a 00 34 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-12T18:49:41Z</CreationTime>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8362	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8366	2	09 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8368	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8408	4	0d 00 0a 00		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA77.tmp.WERInternalMetadata.xml	8412	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBA1.tmp.xml	0	4805	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_EXPORT INVOICE.p_b5f6764852466b593dfad674787e99291849f4a4_5c0e5d72_148dd68c\Report.wer	0	2	fd fd		success or wait	1	7231497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_EXPORT INVOICE.p_b5f6764852466b593dfad674787e99291849f4a4_5c0e5d72_148dd68c\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	185	7231497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_EXPORT INVOICE.p_b5f6764852466b593dfad674787e99291849f4a4_5c0e5d72_148dd68c\Report.wer	14458	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 32 00 30 00 30 00 33 00 30 00 39 00 30 00 32 00 31 00 39 00	MetadataHash=-2003090219	success or wait	1	7231497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	success or wait	1	723336BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	72331FB2	RegCreateKeyExW
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	723143D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	ProgramId	unicode	0006cc3a05750318a8889c88174f9f27b82900000000	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	FileId	unicode	0000ec9de894d7cb09ed3940db31dfc7a39cc1280acd	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	LowerCaseLongPath	unicode	c:\users\user\desktop\export invoice.pdf.exe	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	LongPathHash	unicode	export invoice.p|5cd7ebb	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	Name	unicode	export invoice.pdf.exe	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	Publisher	unicode	havy alegria	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	Version	unicode	1.0.0.0	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	BinFileVersion	unicode	1.0.0.0	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	BinaryType	unicode	pe32_clr_32	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	ProductName	unicode	innoextractor	success or wait	1	723336BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	ProductVersion	unicode	1.0.0.0	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	LinkDate	unicode	05/11/2022 17:26:28	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	BinProductVersion	unicode	1.0.0.0	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	Size	B	00 56 0C 00 00 00 00 00	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	Language	dword	0	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	IsPeFile	dword	1	success or wait	1	723336BF	unknown
\REGISTRY\A\{3f377021-272a-6343-e73e-9fe31aa2b197}\Root\InventoryApplicationFile\export invoice.p|5cd7ebb	IsOsComponent	dword	0	success or wait	1	723336BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 22 D7 C7 73 05 00 00 00 04 16 13 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 AD 6D F8 21 41 01 F4 EA 35 01 01 00 00 00 CF A3 B6 6D D4 EA 35 01 14 C0 29 03 A0 B7 3F 01 80 EA 35 01 5C EA 35 01 00 EA 35 01	success or wait	1	72331FE8	RegSetValueExW

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

Disassembly

No disassembly