ID: 800793
Sample Name:
SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe
Cookbook: default.jbs
Time: 19:58:56
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

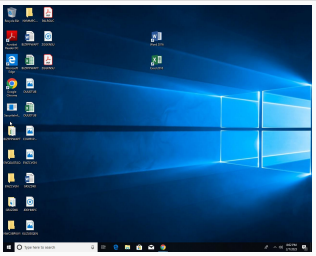
Windows Analysis Report

SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe

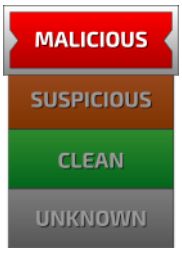
Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe
Analysis ID:	800793
MD5:	bd13975abc6a…
SHA1:	154e70c51508…
SHA256:	7bda9944d4b4…
Tags:	exe
Infos:	



Detection

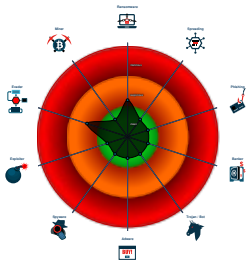


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Uses 32bit PE files
- AV process strings found (often use…
- PE file does not import any functions
- One or more processes crash
- PE file contains an invalid checksum
- Uses code obfuscation techniques (…
- Checks if the current process is bei…
- Contains functionality to access loa…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe (PID: 5948 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe MD5: BD13975ABC6AC3E5A97706A45F48F7DF)
  - WerFault.exe (PID: 6040 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5948 -s 220 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5772 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5948 -s 220 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

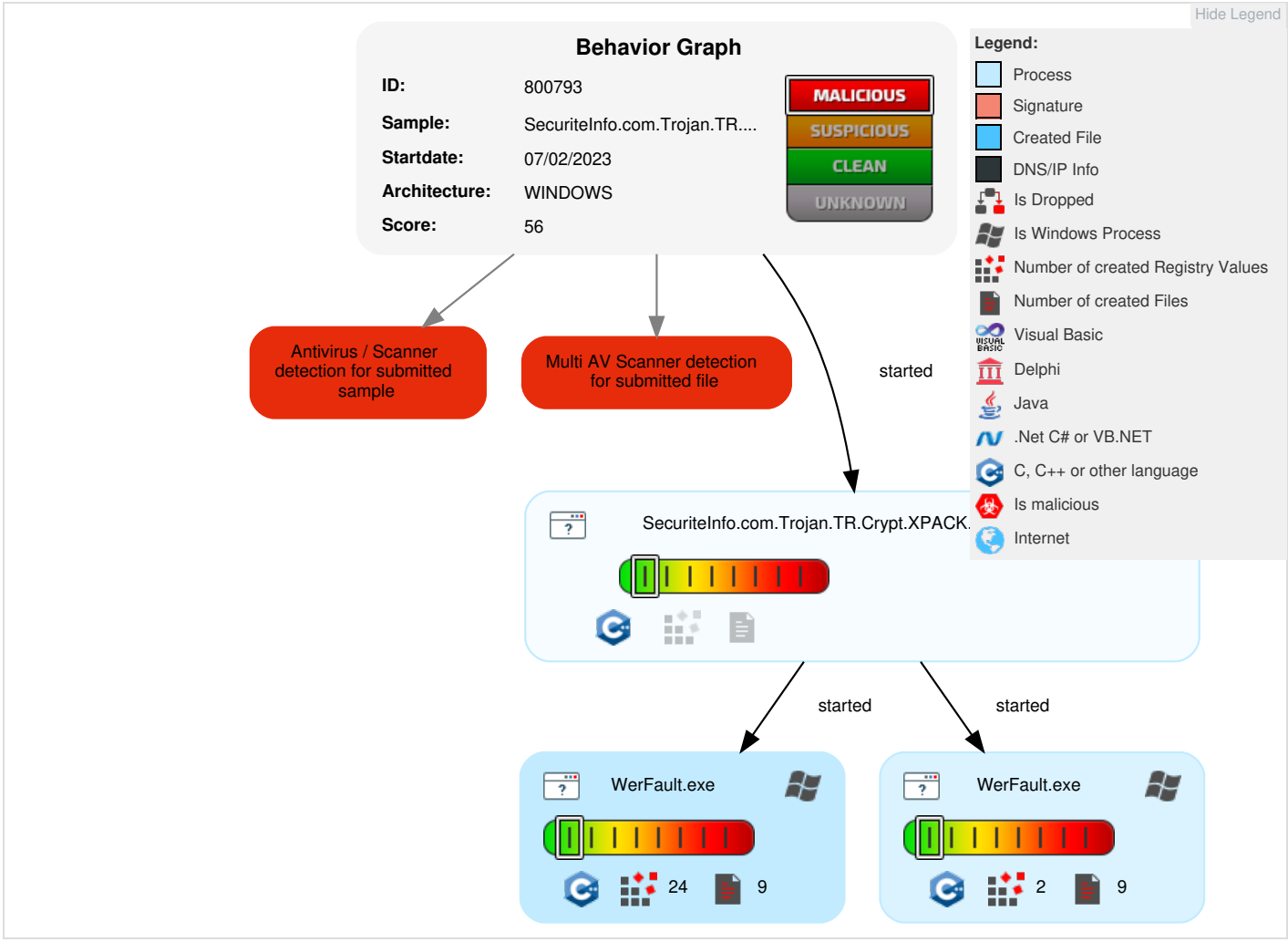
Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

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 Virtualization/Sandbox Evasion	OS Credential Dumping	2 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 Process Injection	LSASS Memory	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)	1 Obfuscated Files or Information	Security Account Manager	1 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)	Binary Padding	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

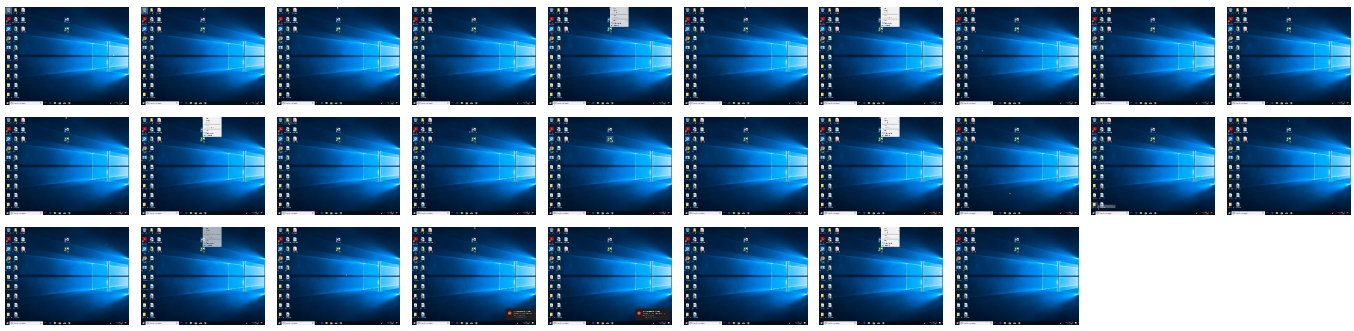
Behavior Graph



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
SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe	13%	ReversingLabs		
SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe	100%	Avira	TR/Crypt.XPACK.Gen	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.clamav.net	SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe	false		high
http://upx.sf.net	Amcache.hve.3.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800793
Start date and time:	2023-02-07 19:58:56 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	16
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
Sample file name:	SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe
Detection:	MAL
Classification:	mal56.winEXE@3/10@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 23%) • Quality average: 19.5% • Quality standard deviation: 36.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.42.73.29, 13.89.179.12
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, ctldl.windowsupdate.com, watson.telemetry.microsoft.com, onedsblobprdcus17.centralus.cloudapp.azure.com
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe

Simulations

Behavior and APIs

No simulations

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_SecuriteInfo.com_63a32cbc58eca2f445502337681ea96cbf1e38a6_5c1322d7_17cc865d\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6785938513999892
Encrypted:	false
SSDEEP:	192:eqj19H2YGwHBUZMXUKOjE/u7shS274lt6LG:DR9H2YGYBUZMXUKOjE/u7shX4lt6LG
MD5:	9E6F5F83756A722153DE06DB0296E447
SHA1:	938128D2C7E77AD36D0FDE60E0E156BD5ABDDB75
SHA-256:	49810D9D418FACA0C29426E9D0D040328CCD0145CE8EB0C30BF3BADF70139C90
SHA-512:	7ADAD777C04BDA5F89CC9895CA634870FD38B40BBC0C2D795B9541DB8460688A7013BA878A13C16151D7E87F040EB1D4170A14C2020C38347B76E12E6FC855EA
Malicious:	false
Reputation:	low

Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.2.0.3.0.2.3.9.7.7.0.2.4.7.7.2.....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.=.1.3.3.2.0.3.0.2.3.9.8.3.1.1.7.9.5.2.....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.=.d.b.e.7.0.e.a.a.-.9.c.a.2.-.4.f.a.e.-.b.7.5.1.-.e.d.7.7.0.8.c.4.f.a.3.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.3.d.f.d.7.8.6.-.4.c.5.b.-.4.b.c.8.-.8.9.8.7.-.3.5.0.1.0.e.3.4.e.d.2.9.....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.=.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...T.R...C.r.y.p.t...X.P.A.C.K...G.e.n...2.3.8.6.2...2.3.7.8.8...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.3.c.-.0.0.0.1.-.0.0.1.a.-.9.0.9.3.-.3.c.c.e.7.1.3.b.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.6.e.4.4.4.f.b.3.6.6.f.a.4.3.2.4.0.c.d.5.7.5.d.7.a.5.8.e.1.3.b.3.0.0.0.0.f.f.f.f.!.0.0.0.0.1.5.4.e.7.0.c.5.1.5.0.8.1.5.3.0.8.e.1.7.b.b.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_f8b2f5d487f13ef078ee9e48b4dedc7a1e0c36a_5c1322d7_16d906f7\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6890775397208573
Encrypted:	false
SSDEEP:	192:8zj19H2YlyOHK5S5KOjE/u7sGS274lt6LG:QR9H2YlyGK5S5KOjE/u7sGX4lt6LG
MD5:	53685A419CF7EC9EEB8E8B262B84AB14
SHA1:	664EB1A851BEE5C233134192608 31F03DDEFD44A
SHA-256:	16706EECDC267A278870AEA6F43800D7FFBCAAAF1AADE5B3411689A9F186B983
SHA-512:	5F79E1FA7C6538F3D0CDF2607FFD7F73107BA54998AEB247ECDCA23E347649C19116420CF603DC6E3367794412610DEC3E3114DBC3583641C11AB3E90E1F6BE
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.2.0.3.0.2.4.3.2.5.7.8.9.8.1.2.....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.=.1.3.3.2.0.3.0.2.4.3.3.1.2.5.8.6.0.1.....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.=.9.a.6.6.a.5.d.7.-.3.9.b.c.-.4.7.e.f.-.8.5.c.b.-.b.8.5.d.3.3.7.7.9.9.1.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.b.3.d.2.0.6.c.-.d.f.3.7.-.4.7.8.4.-.a.b.b.0.-.0.e.f.c.1.2.6.6.6.5.b.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...T.R...C.r.y.p.t...X.P.A.C.K...G.e.n...2.3.8.6.2...2.3.7.8.8...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.3.c.-.0.0.0.1.-.0.0.1.a.-.9.0.9.3.-.3.c.c.e.7.1.3.b.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.6.e.4.4.4.f.b.3.6.6.f.a.4.3.2.4.0.c.d.5.7.5.d.7.a.5.8.e.1.3.b.3.0.0.0.0.f.f.f.f.!.0.0.0.0.1.5.4.e.7.0.c.5.1.5.0.8.1.5.3.0.8.e.1.7.b.b.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 8 04:00:32 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	18004
Entropy (8bit):	2.184282510089021
Encrypted:	false
SSDEEP:	96:548i5X8Q/ZtaLyR9ii7kw4QTnHS44XbX5v9FtZSXJgI9WInWIXQIwLQ0+JSa:Ji5bZtyk9iOQd5vlZMJgvLv+JSa
MD5:	2F9CBFAF66514F6F949E2DA828278CF1
SHA1:	4ED77862C2ED12163C281022D7BF71CDD4861424
SHA-256:	2C2259EFDA83A91C63F67A22DBB273E23FA0196CF8CEC79886A16EA6D2B31759
SHA-512:	2D16BF8D36FFD0E6BB3409CECF443E1BCD0E2867313D04E81541168F79E18E1DB9834A743023A757886DC8AB291C3B9DE56AAD6B3C65AEA477975F9B5DF01D4B
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....`..c.....4..... ...<.....D...I.....T.....8.....T.....=.....\.....H.....U.....B.....GenuineIntelW.....T.....<...<..c.....0..2.....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\WER284.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8584
Entropy (8bit):	3.7190717986753423
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipmla6Q36YAPSUoYfpgmf9VYXS7CpDR89b+RwsfcqmRrlsNipmI6Q36YYSUVxgmf9mXSV+1fA
MD5:	C216304369B0861C406CD0E8BF90B9C9
SHA1:	F4D169D2A08B632CA02F68D4F495DBAC9C6ED0B4
SHA-256:	FB31C1BECD68341E91C0CA0F6D920106E7766B84B69913C88B8C3EA9A1027A12
SHA-512:	8E2E0F499E638C4B39D302BBA012FC804370E7A147E6489E83F24670BA6E251E61EC098CB7029205DD8FFFD8F6C66D94A42F41AC6388BA69160153877808588B
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.>.5.9.4.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E2.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4925
Entropy (8bit):	4.666777965909841
Encrypted:	false
SSDEEP:	48:cvIwSD8zsbJgtWI9lxWgc8sqYjN8fm8M4JK+PFs6+q81PqntU1+xcd:uITf1eggrsqYuJVTtU1+xcd
MD5:	B91254BEBC2CB3BBCC3C2FD371C19BCD
SHA1:	0AF037B5BACAC11F3A80D9806B508BAE5A3BD476
SHA-256:	4E143D383879AB8AF86555DDB5A14E556CE8B072DA21F021BD03AFABDE3A1185
SHA-512:	F1532FBCFEB9CB14037B9724395DB886EBF29F8FB6527BE9F3589D666AB044721482160C35852CA933B43F7A302B84544D2C461C353FB680E6C32B6B49709860
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="1903031" />.. <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" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 8 03:59:57 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	18136
Entropy (8bit):	2.2063334751789574
Encrypted:	false
SSDEEP:	96:5F8igX8Q/vyRCp+ii7kHX/uSOz7244XbXtv9NtZSXWI9WInWIXQI4bCSGq1r4:8igbvkY+iOYGgtvNZMWXbCG1r4
MD5:	D863407F220D9FCD294967B7B3A22500
SHA1:	9D89BA50795E74E905744C983121466734A9476E
SHA-256:	E9873D794BA3AB454452DBE67EB39D5438A29AD201AE1C2828C3CABA4B851205
SHA-512:	12449996E5505F14AD65EC7EFEB172835D2C471EA584B981A76EC08B47BA361089611ABB0856A28D0D5876E25BF86FD7ADB42B089EF10AE2F2A2AE24A8857536
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....=..c.....4..... ...<.....T...I.....T.....8.....T.....>.....\.....H.....U.....B.....GenuineIntelW.....T.....<...<..c.....0..2.....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\WER7AA6.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8482
Entropy (8bit):	3.7119871307963144
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipmlN6ii6YAKSUdhgmf9VXSiCprN89beRwsfZqm:RrlsNipmP6ii6YdSUdhgmf9VSwe1f1
MD5:	64BECBF4071943E2B8CD287D5DCEBA86
SHA1:	B886DA8B4862216F5F1BA7D3E8910506AD91DA1C
SHA-256:	052FBCEC73916EFFE070CEC471F8408E2F0A3006EC9A7F305C492B29631387A2
SHA-512:	B997E14E220F537522D947456A77C0D1535310C729F340F4D1BC53A3459423ACC7B7721199D5EEE2B2B57B09CE61612F62D0900F556C04625F4E401086DC29CF
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.>.5.9.4.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B15.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4827
Entropy (8bit):	4.614432447858704
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6tJgtWl9lxWgc8sqYjz8fm8M4JKvZFaXA+q8+fQntU1+xcd:uITf6HeggrsqYUJQ+Qb+tU1+xcd
MD5:	CDEA9895AE45FAA2B9145C5C8277D26B
SHA1:	09D422C225D41E09692A2934E47959B7AC92E608
SHA-256:	9BB95FD6833B02A12E68F8CF95AB581F45CD1D404768FB9AEA4BAC64E3A09DF1
SHA-512:	6DE03DE585C08C738A8CA1EAAB0DF952D708B02DF995DAEF14BA35396C824BAE1969805BF8B0D6B69A751A817DECBDB47B812DACDE11F0EA1E3A6F257F60F9E5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1903030" />.. <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" />..

C:\Windows\appcompat\Programs\Amcache.hve

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.289519862686535
Encrypted:	false
SSDEEP:	12288:+JgdyhLVs1tqONcKyQL0gGJiBpoIbM6yvUVD1quejGjL+GEkyP:k2yhLVs1tqONcKMBUo6
MD5:	8F475F956A1FDD12DB994C03ED7E6F23
SHA1:	0E3C19098B8C41C4AD1DCD78DB9FB80F0366081A
SHA-256:	F3C1A9728423119F5C89F7B63A644156E106D0A509B030FBC58D1D936AF6C2BA
SHA-512:	02026AE0107171BFF194BE972531CB3F71C24DED5FEEDE8085A841AD4416C6ABB587C22024635ADC28380A6304049AA25F3760E5696EA13AC31FAB9E3B2D1096
Malicious:	false
Preview:	regf_..._...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.*..q;..... ....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.0177781802530625
Encrypted:	false
SSDEEP:	384:2q85SnX9SaPySp9sJImYwSxrZK/MFsJImYwSD:7KStSaPBpWzYwSNZK/dzYwS
MD5:	CA4E9267CF91757F5744DD8FF9324565
SHA1:	C24424A4F80676739C5ACFFED25A9E9583633320
SHA-256:	4726BCB33D0EDE6651D680A10581DA4DC78300259B0CABD83298C0DA94B1B141
SHA-512:	757E694FB09A82E16990AFCB3A52EE2549505AE88E4741591168B4B5A75B0BDE8C2C659D10178249427E7254873395FF7C6BC7EC00767BBB367F5F5B5A7675A5
Malicious:	false

Preview:	regf^...^...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.*..q;..... ....HvLE.>.....^.....Z3.)z.|.S.....0.....hbin.....p.\..,.....nk,....q;..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .....q;..... .....8~..... .....Z.....Root.....lf.....Root....nk .....q;..... .....*.....DeviceCensus..... ..vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.8855949580269264
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe
File size:	188416
MD5:	bd13975abc6ac3e5a97706a45f48f7df
SHA1:	154e70c5150815308e17bbb74cae4ee79948e438
SHA256:	7bda9944d4b4a62a86088d56ad964c0a4b98516c93f6467cd89a8f8f655a0029
SHA512:	9fee403e82536f4c3c42225762e2ebd1c66496fb94ca1b97ccdc11ced2e56211e60159d6b183667a8fdf270faec42d31888ef60be0f1e401f5d12fb976732178
SSDEEP:	3072:jCY64XFREi9URWKznfMvJ/zl6HvK2KkAtZodTzHHNaTrOT:tTORmLyJdvH4TrOT
TLSH:	EB046C316842A495F0E3E8F3C9EBD47DBB0977A0030224F761CC065AA7625FA763E553
File Content Preview:	MZ.....@.....!.L.!This file was created by ClamAV for internal use and should not be run...ClamAV - A GPL virus scanner - http://www.clamav.net..$...PE..L...CLAM..... .....k.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41856b
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x4D414C43 [Thu Jan 27 10:43:15 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 004234E8h
push 0041CA40h

Instruction
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
sub esp, 58h
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp
call dword ptr [004230CCh]
xor edx, edx
mov dl, ah
mov dword ptr [0042C508h], edx
mov ecx, eax
and ecx, 000000FFh
mov dword ptr [0042C504h], ecx
shl ecx, 08h
add ecx, edx
mov dword ptr [0042C500h], ecx
shr eax, 10h
mov dword ptr [0042C4FCh], eax
push 00000001h
call 00007F3F2A4A3236h
pop ecx
test eax, eax
jne 00007F3F58A4312Ah
push 0000001Ch
call 00007F3EED1A3236h
pop ecx
call 00007F3FD0723236h
test eax, eax
jne 00007F3F58A4312Ah
push 00000010h
call 00007F3EED1A3236h
pop ecx
xor esi, esi
mov dword ptr [ebp-04h], esi
call 00007F3F1EF73236h
call dword ptr [004230C8h]
mov dword ptr [0042CB34h], eax
call 00007F3F9E713236h
mov dword ptr [0042C560h], eax
call 00007F3F516E3236h
call 00007F3F986E3236h
call 00007F3EDFF43236h
mov dword ptr [ebp-30h], esi
lea eax, dword ptr [ebp-5Ch]
push eax
call dword ptr [00423088h]
call 00007F3F406D3236h
mov dword ptr [ebp-64h], eax
test byte ptr [ebp-30h], 00000001h
je 00007F3F58A43128h
movzx eax, word ptr [ebp+00h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x23f88	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x23000	0x1a8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

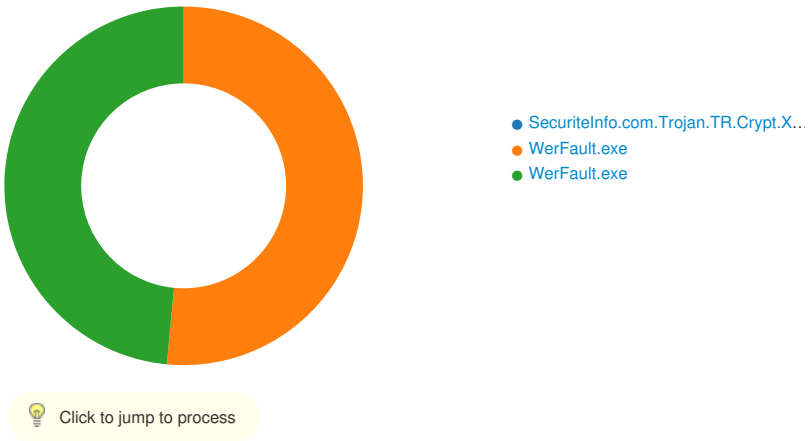
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x22000	0x22000	False	0.4499942555147059	data	6.458075836010223	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x23000	0x2000	0x2000	False	0.2213134765625	data	2.8987922797855528	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x25000	0x9000	0x9000	False	0.20203993055555555	data	3.054353288110077	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe PID: **5948**, Parent PID: **3320**

General

Target ID:	0
Start time:	19:59:56
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe
Imagebase:	0x400000
File size:	188416 bytes
MD5 hash:	BD13975ABC6AC3E5A97706A45F48F7DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: **6040**, Parent PID: **5948**

General

Target ID:	3
Start time:	19:59:56
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5948 -s 220
Imagebase:	0x80000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CE31717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B15.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B15.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE2497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_63a32cbc58eca2f445502337681ea96cbf1e38a6_5c1322d7_17cc865d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_63a32cbc58eca2f445502337681ea96cbf1e38a6_5c1322d7_17cc865d\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE2497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B15.tmp	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B15.tmp.xml	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B13.tmp.csv	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BDF.tmp.txt	success or wait	1	6CE2497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 3d 1e fd 63 fd 05 12 00 00 00 00 00	MDMP =c	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	3040	6	00 00 00 00 00 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.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 fd 0b 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 3c 17 00 00 3c 1e fd 63 00 00 00 00 00 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 32 00 00 00 00 00 00 00 01 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 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 00 00 00	UBGenuineIntelWT<<c02 Pacific Standard TimePacific Daylight Time	success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	3284	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 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 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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 6b fd 41 00 6b fd 41 00 00 fd 23 00 6b fd 41 00 6b fd 41 00 fd fd 19 00 fd fd 19 00 00 00 00 00 23 00 00 00 16 02 01 00 08 fd 19 00 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	+S++kAkA#kAkA#+	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	1620	168	34 17 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 0c 00 00	4	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	4716	20	05 00 00 00 3c fd fd 77 00 00 00 00 00 01 00 00 fd 12 00 00	<w	success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	4800	256	fd 08 00 fd fd 54 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 55 00 00 00 fd fd fd fd 77 fd fd fd 2c 00 fd fd 56 00 00 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 57 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 58 00 00 00 fd fd fd fd 77 fd fd fd 0c 00 fd fd 59 00 00 00 fd fd fd fd 77 fd fd fd 40 00 fd fd 5a 00 18 00 fd fd fd fd 77 fd fd fd 04 00 fd fd 5b 00 1d 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 5c 00 00 00 fd fd fd fd 77 fd fd fd 10 00 fd fd 5d 00 00 00 fd fd fd fd 77 fd fd fd 08 00 fd fd 5e 00 00 00 fd fd fd fd 77 fd fd fd 10 00 fd fd 5f 00 00 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 60 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 61 00 07 00 fd fd fd fd 77 fd fd fd 08 00 fd fd 62 00 00 00 fd fd fd fd 77 fd fd fd 1c 00 fd fd 63 00 00 00 fd fd fd fd 77 fd	TwUw,VwWwXwYw@Zw[w\w]w^w_w`wawbwcw	success or wait	4	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	10332	4212	fd fd fd 77 fd 1a 6f 77 fd fd fd fd fd fd 19 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 00 00 00 fd 00 00 00 00 00 00 00 24 00 00 00 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 00 00 fd fd fd fd 00 fd 23 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wow$#	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	1788	4	01 00 00 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	4000	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 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 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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 6b fd 41 00 6b fd 41 00 00 00 00 00 20 fd 19 00 fd fd fd 77 23 00 00 00 16 02 00 00 fd fd 19 00 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++kAkA w#+	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	1792	48	34 17 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 10 24 00 00 00 00 00 fd fd 19 00 00 00 00 00 74 10 00 00 5c 28 00 00 fd 02 00 00 fd 0f 00 00	4 $t\(	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	1852	4	05 00 00 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	3046	122	74 00 00 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 54 00 52 00 2e 00 43 00 72 00 79 00 70 00 74 00 2e 00 58 00 50 00 41 00 43 00 4b 00 2e 00 47 00 65 00 6e 00 2e 00 32 00 33 00 38 00 36 00 32 00 2e 00 32 00 33 00 37 00 38 00 38 00 2e 00 65 00 78 00 65 00 00 00	tSecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe	success or wait	5	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	2288	752	00 00 3d 74 00 00 00 00 00 fd 09 00 fd fd 09 00 51 fd 0f fd fd 0c 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 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 fd 14 03 00 00 00 00 fd 7a 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 77 03 00 00 00 00 00 27 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1b 00 00 00 00 00 fd 78 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 04 00 00 00 00	=tQBB?$@AZbzw'x@	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	14544	3592	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	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER79AB.tmp.dmp	32	108	03 00 00 00 34 00 00 00 fd 06 00 00 04 00 00 00 20 02 00 00 3c 07 00 00 05 00 00 00 54 00 00 00 6c 12 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 08 00 00 08 3e 00 00 15 00 00 00 fd 01 00 00 5c 09 00 00 16 00 00 00 fd 00 00 00 48 0b 00 00	4 <TIT8T>\H	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 34 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5948</Pid>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1002	162	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 54 00 52 00 2e 00 43 00 72 00 79 00 70 00 74 00 2e 00 58 00 50 00 41 00 43 00 4b 00 2e 00 47 00 65 00 6e 00 2e 00 32 00 33 00 38 00 36 00 32 00 2e 00 32 00 33 00 37 00 38 00 38 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>SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe</ImageName>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1164	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1168	2	09 00		success or wait	2	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1172	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>00000000</CmdLineSignature>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1262	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1266	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1270	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 37 00 39 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1796</Uptime>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1320	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1402	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1406	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1410	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1462	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1466	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1470	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1514	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1518	2	09 00		success or wait	3	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1524	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 37 00 30 00 39 00 32 00 36 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>17092608</PeakVirtualSize>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1610	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1614	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1620	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 31 00 33 00 31 00 37 00 37 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>13131776</VirtualSize>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1690	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1694	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1700	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 38 00 32 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>829</PageFaultCount>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1772	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1776	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1782	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 30 00 34 00 33 00 33 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3043328</PeakWorkingSetSize>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1878	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1882	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1888	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 30 00 34 00 33 00 33 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3043328</WorkingSetSize>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1968	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1972	2	09 00		success or wait	3	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	1978	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 32 00 34 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>32432</QuotaPeakPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2090	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2094	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2100	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 35 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>24520</QuotaPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2196	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2200	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2206	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 30 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>8088</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2328	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2332	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2338	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 38 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>7816</QuotaNonPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2444	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2448	2	09 00		success or wait	3	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2454	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 31 00 36 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>581632</PagefileUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2528	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2532	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2538	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 39 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>589824</PeakPagefileUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2628	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2632	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2638	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 31 00 36 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>581632</PrivateUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2708	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2712	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2716	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2762	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2766	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2770	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2810	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2850	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2854	2	09 00		success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2862	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3320</Pid>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2904	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2974	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2978	2	09 00		success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	2986	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3088	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 35 00 33 00 34 00 34 00 39 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5534493</Uptime>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3136	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3140	2	09 00		success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3148	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3226	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3230	2	09 00		success or wait	4	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3238	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3302	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3346	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3350	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3360	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3450	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3454	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3464	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3538	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3542	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3552	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 35 00 35 00 37 00 36 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>55766</PageFaultCount>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3628	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3632	2	09 00		success or wait	5	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3642	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 32 00 31 00 38 00 38 00 38 00 37 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121888768</PeakWorkingSetSize>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3742	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3746	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3756	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 32 00 31 00 38 00 37 00 36 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>121876480</WorkingSetSize>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3840	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3844	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3854	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 34 00 32 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>1142160</QuotaPeakPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3970	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3974	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	3984	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 38 00 31 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1081168</QuotaPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4084	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4088	2	09 00		success or wait	5	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4098	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 39 00 32 00 34 00 39 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>92496</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4222	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4226	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4236	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 39 00 39 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>79936</QuotaNonPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4344	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4348	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4358	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 35 00 33 00 36 00 37 00 32 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>45367296</PagefileUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4436	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4440	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4450	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 36 00 38 00 32 00 31 00 33 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>46821376</PeakPagefileUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4544	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4548	2	09 00		success or wait	5	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4558	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 35 00 33 00 36 00 37 00 32 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>45367296</PrivateUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4632	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4636	2	09 00		success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4644	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4690	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4694	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4700	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4742	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4746	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4750	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4782	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4786	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4788	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4830	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4834	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4836	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4874	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4878	2	09 00		success or wait	2	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4882	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4944	4	0d 00 0a 00		success or wait	8	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4948	2	09 00		success or wait	16	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	4952	166	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 54 00 52 00 2e 00 43 00 72 00 79 00 70 00 74 00 2e 00 58 00 50 00 41 00 43 00 4b 00 2e 00 47 00 65 00 6e 00 2e 00 32 00 33 00 38 00 36 00 32 00 2e 00 32 00 33 00 37 00 38 00 38 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>SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe</Parameter0>	success or wait	8	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	5684	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	5688	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	5690	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	5730	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	5734	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	5736	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	5774	4	0d 00 0a 00		success or wait	6	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	5778	2	09 00		success or wait	12	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	5782	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6336	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6340	2	09 00		success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6342	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6382	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6386	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6388	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6426	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6430	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6434	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6528	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6532	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6536	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 63 00 63 00 76 00 75 00 66 00 6f 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>ccvufo, Inc.</SystemManufacturer>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6642	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6646	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6650	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 63 00 76 00 75 00 66 00 6f 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>ccvufo7,1</SystemProductName>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6746	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6750	2	09 00		success or wait	2	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6754	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6874	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6878	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6882	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 36 00 31 00 34 00 33 00 36 00 34 00 39 00 36 00 31 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>1614364961</OSInstallDate>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6964	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6968	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	6972	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7074	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7078	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7082	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7150	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7154	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7156	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7196	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7200	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7202	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7236	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7240	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7244	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7340	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7344	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7346	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7382	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7386	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7388	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7412	4	0d 00 0a 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7416	2	09 00		success or wait	6	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7420	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7664	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7668	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7670	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7696	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7700	2	09 00		success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7702	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 33 00 2d 00 30 00 32 00 2d 00 30 00 38 00 54 00 30 00 33 00 3a 00 35 00 39 00 3a 00 35 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-02-08T03:59:57Z">	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7802	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7806	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	7810	254	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 32 00 39 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 39 00 34 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 39 00 33 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 39 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22 00 3e 00	<Process AsId="295" PID="5948" UptimeMS="93" TimeSinceCreationMS="93" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1">	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8064	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8068	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8072	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8092	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8096	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8098	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8136	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8140	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8142	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	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8180	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8184	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8188	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 62 00 65 00 37 00 30 00 65 00 61 00 61 00 2d 00 39 00 63 00 61 00 32 00 2d 00 34 00 66 00 61 00 65 00 2d 00 62 00 37 00 35 00 31 00 2d 00 65 00 64 00 37 00 37 00 30 00 38 00 63 00 34 00 66 00 61 00 33 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>dbe70eaa-9ca2-4fae-b751-ed7708c4fa37</Guid>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8286	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8290	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8294	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 33 00 2d 00 30 00 32 00 2d 00 30 00 38 00 54 00 30 00 33 00 3a 00 35 00 39 00 3a 00 35 00 37 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>2023-02-08T03:59:57Z</CreationTime>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8392	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8396	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8398	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8438	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AA6.tmp.WERInternalMetadata.xml	8442	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	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B15.tmp.xml	0	4827	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 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 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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_63a32cbc58eca2f445502337681ea96cbf1e38a6_5c1322d7_17cc865d\Report.wer	0	2	fd fd		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_63a32cbc58eca2f445502337681ea96cbf1e38a6_5c1322d7_17cc865d\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	129	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_63a32cbc58eca2f445502337681ea96cbf1e38a6_5c1322d7_17cc865d\Report.wer	8076	42	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 38 00 32 00 34 00 32 00 31 00 33 00 30 00 38 00	MetadataHash=82421308	success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	success or wait	1	6CE436BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6CE41FB2	RegCreateKeyExW
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE243D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	ProgramId	unicode	00066e444fb366fa43240cd575d7a58e13b30000ffff	success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	FileId	unicode	0000154e70c5150815308e17bbb74cae4ee79948e438	success or wait	1	6CE436BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	LowerCaseLongPath	unicode	c:\users\user\desktop\securiteinfo.com.trojan.tr.crypt.xpack.gen.23862.23788.exe	success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	LongPathHash	unicode	securiteinfo.com|ff1fbb3f	success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	Name	unicode	securiteinfo.com.trojan.tr.crypt.xpack.gen.23862.23788.exe	success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	Publisher	unicode		success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	Version	unicode		success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	BinFileVersion	unicode		success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	BinaryType	unicode	pe32_i386	success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	ProductName	unicode		success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	ProductVersion	unicode		success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	LinkDate	unicode	01/27/2011 10:43:15	success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	BinProductVersion	unicode		success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	Size	B	00 E0 02 00 00 00 00 00	success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	Language	dword	0	success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	IsPeFile	dword	1	success or wait	1	6CE436BF	unknown
\REGISTRY\A\{93131b2d-1a6a-440d-72e0-9cc353075f27}\Root\InventoryApplicationFile\securiteinfo.com|ff1fbb3f	IsOsComponent	dword	0	success or wait	1	6CE436BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CE41FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 5772, Parent PID: 5948

General

Target ID:	12
Start time:	20:00:32
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5948 -s 220
Imagebase:	0x80000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CE31717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E2.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_f8b2f5d487f13ef078ee9e48b4dedc7a1e0c36a_5c1322d7_16d906f7	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_f8b2f5d487f13ef078ee9e48b4dedc7a1e0c36a_5c1322d7_16d906f7\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CE2497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E2.tmp	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E2.tmp.xml	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E2.tmp.csv	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3AF.tmp.txt	success or wait	1	6CE2497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 60 1e fd 63 fd 05 12 00 00 00 00 00	MDMP `c	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	3040	6	00 00 00 00 00 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.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 fd 0b 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 3c 17 00 00 3c 1e fd 63 00 00 00 00 00 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 32 00 00 00 00 00 00 00 01 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 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	UBGenuineIntelWT<<c02 Pacific Standard TimePacific Daylight T ime	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	3284	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 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 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 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 70 fd 19 00 fd fd fd 77 40 fd 41 00 78 fd 19 00 fd fd 19 00 fd fd fd fd 23 00 00 00 02 02 01 00 7c fd 19 00 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++pw@Ax#|+	success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	1620	168	34 17 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 02 00 00 fd 0c 00 00	4	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	4716	20	04 00 00 00 00 fd 23 00 00 00 00 00 fd 04 00 00 fd 12 00 00	#	success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	4784	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 fd 0a 49 00 00 00 00 00 00 00 49 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 01 00 01 00 00 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 01 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@{wIlyw{w0(Pm `fwPSwB	success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	10060	4488	00 00 00 00 fd fd 41 00 70 fd 19 00 fd fd fd fd fd fd 19 00 fd fd 19 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 19 00 52 fd fd 77 78 fd 19 00 70 fd 19 00 fd fd 19 00 24 fd 19 00 70 fd 19 00 fd fd fd 77 70 fd 19 00 fd fd 19 00 24 fd fd 77 78 fd 19 00 70 fd 19 00 fd fd 19 00 24 fd 19 00 40 fd 41 00 78 fd 19 00 fd fd 19 00 70 fd 19 00 51 21 fd 77 78 fd 19 00 70 fd 19 00 fd fd 19 00 24 fd 19 00 40 fd 41 00 fd fd fd fd 00 00 00 00 fd fd 19 00 fd fd fd fd fd fd fd fd fd fd 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ApRwxppwpwxp$@Ax pQ!wxp$@A	success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	1788	4	01 00 00 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	4000	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 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 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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 70 fd 19 00 fd fd fd 77 40 fd 41 00 78 fd 19 00 fd fd 19 00 fd fd fd fd 23 00 00 00 02 02 01 00 7c fd 19 00 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++pw@Ax#|+	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	1792	48	34 17 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 10 24 00 00 00 00 00 78 fd 19 00 00 00 00 00 fd 11 00 00 4c 27 00 00 fd 02 00 00 fd 0f 00 00	4 $xL'	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	1852	4	05 00 00 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	3046	122	74 00 00 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 54 00 52 00 2e 00 43 00 72 00 79 00 70 00 74 00 2e 00 58 00 50 00 41 00 43 00 4b 00 2e 00 47 00 65 00 6e 00 2e 00 32 00 33 00 38 00 36 00 32 00 2e 00 32 00 33 00 37 00 38 00 38 00 2e 00 65 00 78 00 65 00 00 00	tSecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe	success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	2288	752	00 00 3d 74 00 00 00 00 00 fd 09 00 fd fd 09 00 51 fd 0f fd fd 0c 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 14 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 7d 03 00 00 00 00 00 27 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 31 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 01 fd 04 00 00 00 00	=tQBB?$@AZb}'1@	success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	14548	3456	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	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E6.tmp.dmp	32	108	03 00 00 00 34 00 00 00 fd 06 00 00 04 00 00 00 20 02 00 00 3c 07 00 00 05 00 00 00 44 00 00 00 6c 12 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 08 00 00 fd 3d 00 00 15 00 00 00 fd 01 00 00 5c 09 00 00 16 00 00 00 fd 00 00 00 48 0b 00 00	4 <DIT8T=\H	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.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	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 34 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5948</Pid>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1002	162	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 54 00 52 00 2e 00 43 00 72 00 79 00 70 00 74 00 2e 00 58 00 50 00 41 00 43 00 4b 00 2e 00 47 00 65 00 6e 00 2e 00 32 00 33 00 38 00 36 00 32 00 2e 00 32 00 33 00 37 00 38 00 38 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>SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe</ImageName>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1164	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1168	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1172	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1262	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1266	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1270	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 36 00 35 00 37 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>36579</Uptime>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1322	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	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1404	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1408	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1412	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1464	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1468	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1472	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1516	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1520	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1526	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 37 00 30 00 39 00 32 00 36 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>17092608</PeakVirtualSize>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1612	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1616	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1622	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 31 00 32 00 37 00 36 00 38 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>13127680</VirtualSize>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1692	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1696	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1702	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 38 00 33 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>833</PageFaultCount>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1774	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1778	2	09 00		success or wait	3	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1784	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 30 00 35 00 35 00 36 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>3055616</PeakWorkingSetSize>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1890	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 30 00 35 00 31 00 35 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3051520</WorkingSetSize>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1970	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1974	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	1980	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 32 00 34 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>32432</QuotaPeakPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2092	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2096	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2102	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 35 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>24512</QuotaPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2198	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2202	2	09 00		success or wait	3	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2208	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>9224</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2330	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2334	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2340	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 38 00 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>9088</QuotaNonPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2446	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2450	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2456	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 31 00 36 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>581632</PagefileUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2530	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2534	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2540	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 39 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>589824</PeakPagefileUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2630	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2634	2	09 00		success or wait	3	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2640	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 31 00 36 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>581632</PrivateUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2710	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2714	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2718	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2764	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2768	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2772	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2802	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2806	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2812	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2852	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2856	2	09 00		success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2864	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3320</Pid>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2894	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2898	2	09 00		success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2906	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2976	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2980	2	09 00		success or wait	4	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	2988	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3078	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3082	2	09 00		success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3090	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 35 00 36 00 39 00 33 00 32 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5569322</Uptime>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3138	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3142	2	09 00		success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3150	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3240	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3292	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3296	2	09 00		success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3304	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3348	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3352	2	09 00		success or wait	5	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3362	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3452	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3456	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3466	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3540	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3544	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3554	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 35 00 39 00 34 00 34 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>59441</PageFaultCount>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3630	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3634	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3644	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 32 00 32 00 30 00 34 00 38 00 35 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>122048512</PeakWorkingSetSize>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3744	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3748	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3758	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 32 00 32 00 30 00 30 00 30 00 33 00 34 00 35 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>122003456</WorkingSetSize>	success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3842	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3846	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3856	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 34 00 32 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11421 60</QuotaPeakPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3972	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3976	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	3986	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 38 00 30 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1080504</ QuotaPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4086	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4090	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4100	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 39 00 32 00 34 00 39 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>92 496</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4224	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4228	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4238	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 38 00 30 00 37 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>80728< /QuotaNonPagedPoolUsage>	success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4346	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4350	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4360	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 35 00 31 00 33 00 37 00 39 00 32 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>45137920</PagefileUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4438	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4442	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4452	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 36 00 38 00 32 00 31 00 33 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>46821376</PeakPagefileUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4546	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4550	2	09 00		success or wait	5	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4560	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 35 00 31 00 33 00 37 00 39 00 32 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>45137920</PrivateUsage>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4634	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4638	2	09 00		success or wait	4	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4646	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4692	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4696	2	09 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4702	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4744	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4748	2	09 00		success or wait	2	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4752	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4784	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4788	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4790	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4832	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4836	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4838	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4876	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4880	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4884	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4946	4	0d 00 0a 00		success or wait	8	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4950	2	09 00		success or wait	16	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	4954	166	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 54 00 52 00 2e 00 43 00 72 00 79 00 70 00 74 00 2e 00 58 00 50 00 41 00 43 00 4b 00 2e 00 47 00 65 00 6e 00 2e 00 32 00 33 00 38 00 36 00 32 00 2e 00 32 00 33 00 37 00 38 00 38 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>SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe</Parameter0>	success or wait	8	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	5784	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	5788	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	5790	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	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	5830	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	5834	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	5836	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	5874	4	0d 00 0a 00		success or wait	6	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	5878	2	09 00		success or wait	12	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	5882	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6436	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6440	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6442	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6482	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6486	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6488	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6526	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6530	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6534	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6628	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6632	2	09 00		success or wait	2	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6636	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 63 00 63 00 76 00 75 00 66 00 6f 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>ccvufo, Inc.</SystemManufacturer>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6742	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6746	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6750	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 63 00 76 00 75 00 66 00 6f 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>ccvufo7,1</SystemProductName>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6846	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6850	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6854	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6974	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6978	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	6982	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 36 00 31 00 34 00 33 00 36 00 34 00 39 00 36 00 31 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>1614364961</OSInstallDate>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7064	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7068	2	09 00		success or wait	2	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7072	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7174	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7178	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7182	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7250	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7254	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7256	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7296	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7300	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7302	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7336	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7340	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7344	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7440	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7444	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7446	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	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7482	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7486	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7488	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7512	4	0d 00 0a 00		success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7516	2	09 00		success or wait	6	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7520	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 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>80000000</Flags>	success or wait	3	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7766	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7770	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7772	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7798	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7802	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7804	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 33 00 2d 00 30 00 32 00 2d 00 30 00 38 00 54 00 30 00 34 00 3a 00 30 00 30 00 3a 00 33 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-02-08T04:00:32Z">	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7904	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7908	2	09 00		success or wait	2	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	7912	254	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 32 00 39 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 39 00 34 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 39 00 33 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 39 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22 00 3e 00	<Process AsId="295" PID="5948" UptimeMS="93" TimeSinceCreationMS="93" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1">	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8166	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8170	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8174	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8194	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8198	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8200	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8238	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8242	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8244	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8282	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8286	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8290	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 61 00 36 00 36 00 61 00 35 00 64 00 37 00 2d 00 33 00 39 00 62 00 63 00 2d 00 34 00 37 00 65 00 66 00 2d 00 38 00 35 00 63 00 62 00 2d 00 62 00 38 00 35 00 64 00 33 00 33 00 37 00 37 00 39 00 39 00 31 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>9a66a5d7-39bc-47ef-85cb-b85d33779917</Guid>	success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8388	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8392	2	09 00		success or wait	2	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8396	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 33 00 2d 00 30 00 32 00 2d 00 30 00 38 00 54 00 30 00 34 00 3a 00 30 00 30 00 3a 00 33 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-02-08T04:00 :32Z</CreationTime>	success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8494	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8498	2	09 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8500	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8540	4	0d 00 0a 00		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER284.tmp.WERInternalMetadata.xml	8544	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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E2.tmp.xml	0	4925	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 3c 6f 73 3e 0d 0a 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 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 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	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_f8b2f5d487f13ef078ee9e48b4dedc7a1e0c36a_5c1322d7_16d906f7\Report.wer	0	2	fd fd		success or wait	1	6CE2497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_f8b2f5d487f13ef078ee9e48b4dedc7a1e0c36a_5c1322d7_16d906f7\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	130	6CE2497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_f8b2f5d487f13ef078ee9e48b4dedc7a1e0c36a_5c1322d7_16d906f7\Report.wer	8208	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 32 00 30 00 38 00 31 00 36 00 36 00 34 00 30 00 38 00 31 00	MetadataHash=2081664081	success or wait	1	6CE2497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0e5cc852-c71b-21c4-3a90-7050fc7c38dc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE436BF	unknown
\REGISTRY\A\{0e5cc852-c71b-21c4-3a90-7050fc7c38dc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE436BF	unknown
\REGISTRY\A\{0e5cc852-c71b-21c4-3a90-7050fc7c38dc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CE243D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 FD CB FA 86 02 00 00 00 00 00 00 00 FD CB FA 86 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CE41FE8	RegSetValueExW

Disassembly

No disassembly