ID: 756119
Sample Name: SecuriteInfo.com.Win32.PWSX-gen.16188.7094.exe
Cookbook: default.jbs
Time: 16:55:10
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

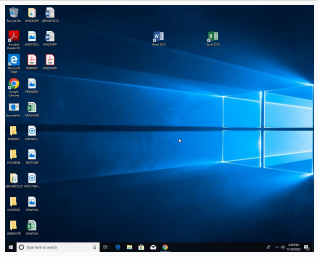
Windows Analysis Report

SecuriteInfo.com.Win32.PWSX-gen.16188.7094.exe

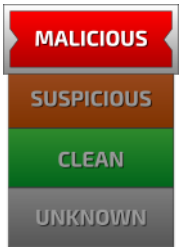
Overview

General Information

Sample Name:	SecuriteInfo.com.Win32.PWSX-gen.16188.7094.exe
Analysis ID:	756119
MD5:	c852376dda1de8..
SHA1:	2377355189c59e..
SHA256:	2c9d6d1a184ed2..
Tags:	exe
Infos:	



Detection

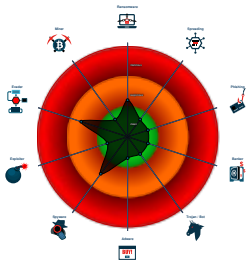


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Machine Learning detection for sam…
- Uses 32bit PE files
- One or more processes crash
- Contains functionality to check if a d…
- Contains functionality to read the PE…
- Uses code obfuscation techniques (…
- Checks if the current process is bei…
- PE file contains sections with non-s…
- Detected potential crypto function
- Contains functionality to query CPU…
- Found potential string decryption / a…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Win32.PWSX-gen.16188.7094.exe (PID: 5640 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.16188.7094.exe MD5: C852376DDA1DE89231D5F558255775E0)
  - WerFault.exe (PID: 5688 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5640 -s 464 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

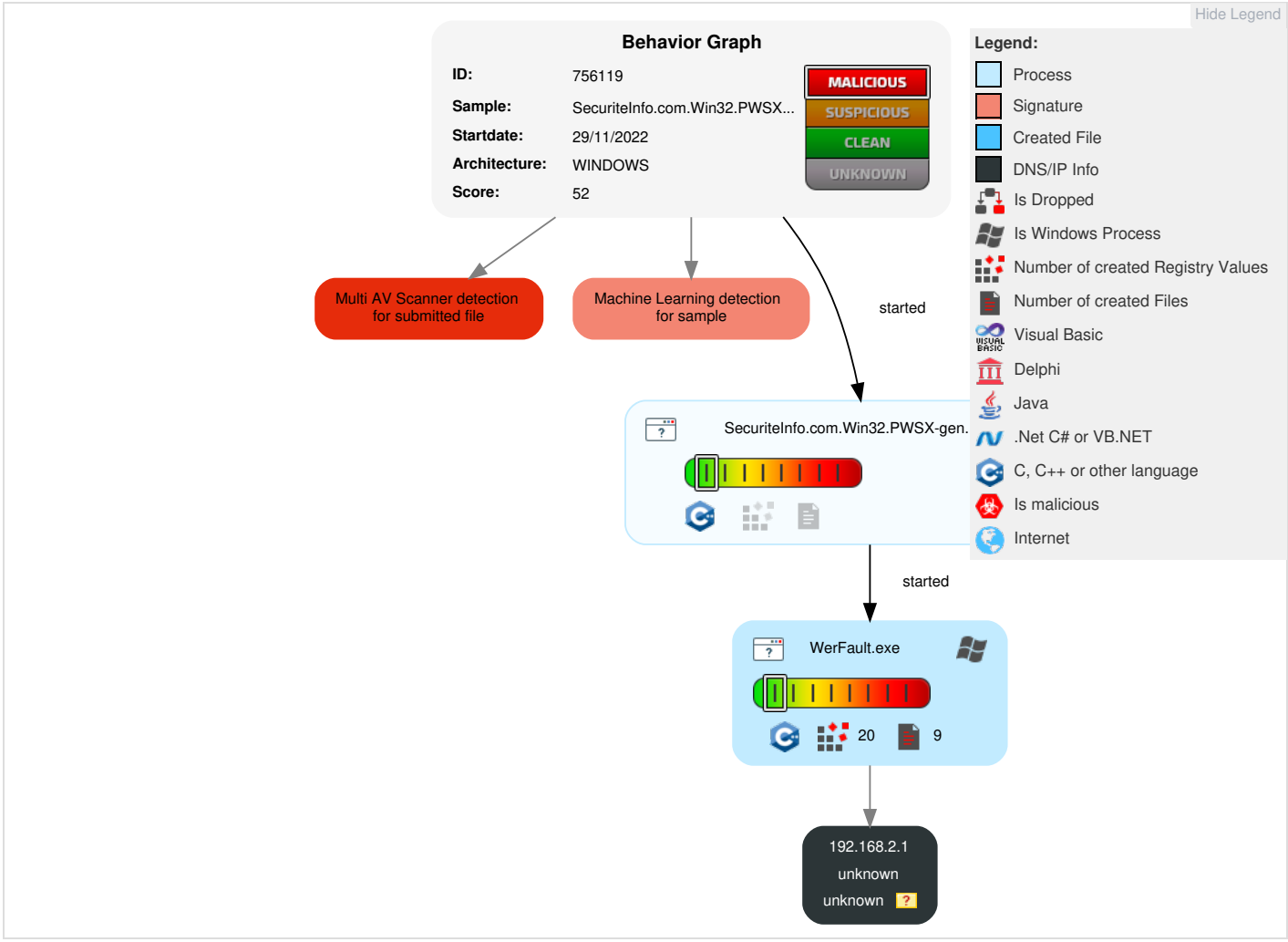
Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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	2 Command and Scripting Interpreter	Path Interception	1 Process Injection	1 Virtualization/Sandbox Evasion	1 1 Input Capture	1 System Time Discovery	Remote Services	1 1 Input Capture	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	3 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	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 Deobfuscate/Decode Files or Information	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Clipboard Data	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

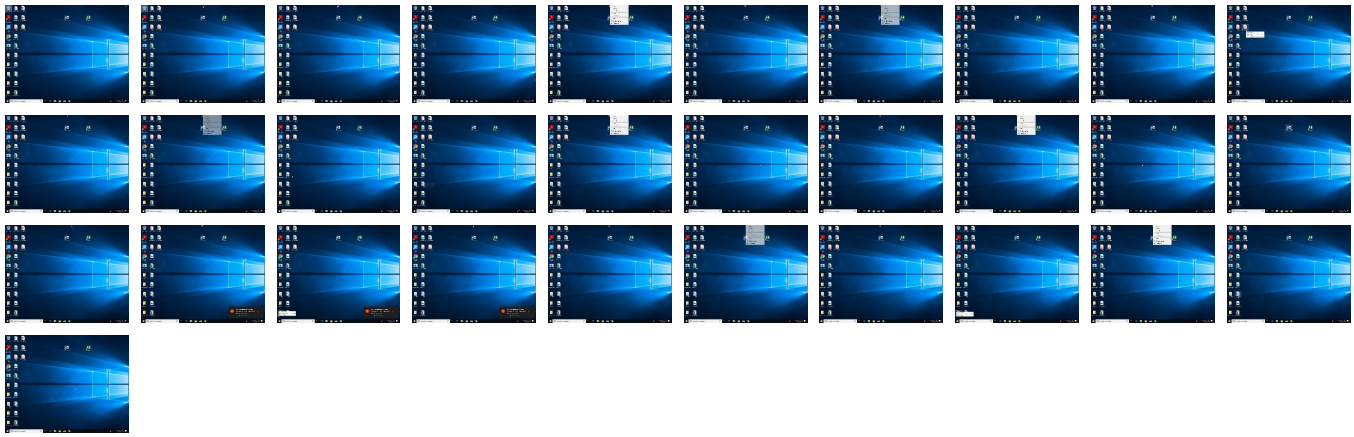
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Win32.PWSX-gen.16188.7094.exe	17%	ReversingLabs	Win32.Trojan.Convagent	
SecuriteInfo.com.Win32.PWSX-gen.16188.7094.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

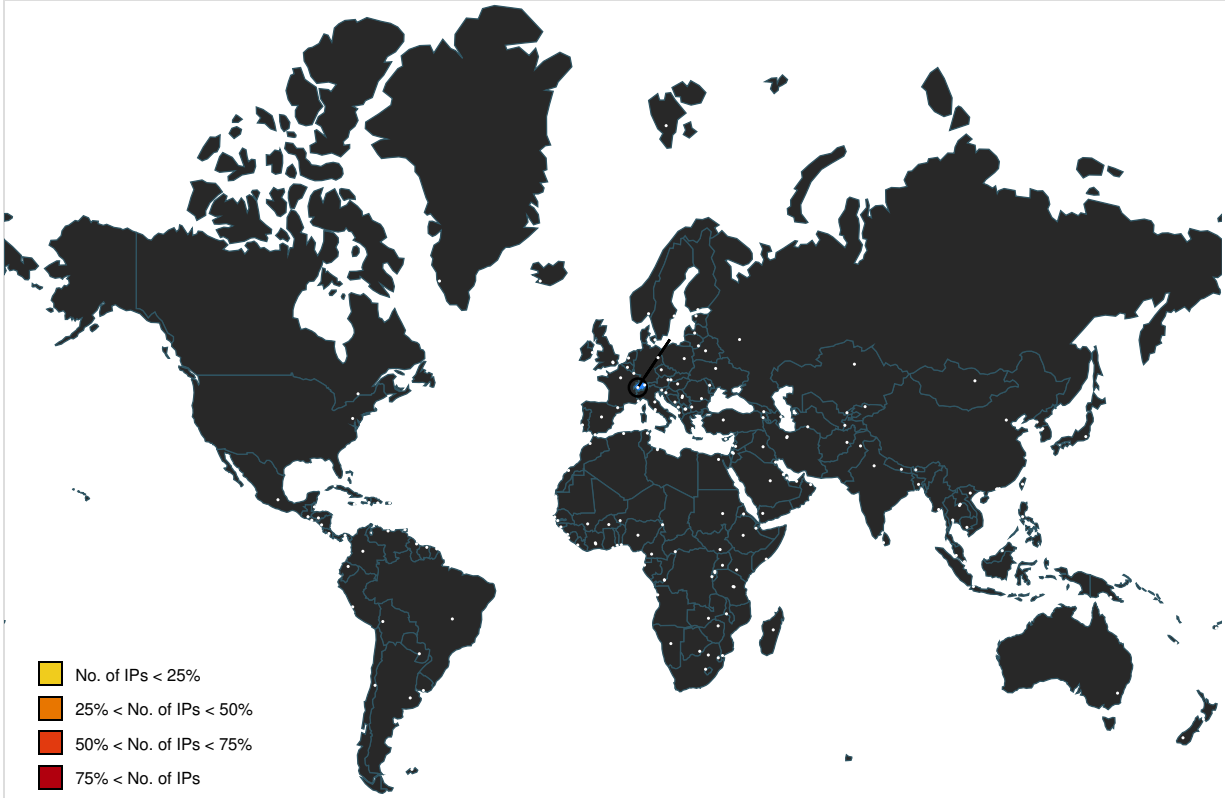
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756119
Start date and time:	2022-11-29 16:55:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win32.PWSX-gen.16188.7094.exe
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.winEXE@2/4@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 78.4%) • Quality average: 66.9% • Quality standard deviation: 40.2%
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): 20.42.65.92
- Excluded domains from analysis (whitelisted): fs.microsoft.com, onedsblobprdeus17.eastus.cloudapp.azure.com, blobcollector.events.data.trafficmanager.net, ctldl.windowsupdate.com, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information

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_c136f9839aaccad85a66b9f733bbb3cf4c588e0_e9cd6a7e_166ff3ee\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):	0.8714732038462919
Encrypted:	false
SSDEEP:	96:QrxoFzqgLj9UhO9e77f5pXIQcQvc6QcEDMcw3Diji+HbHg/EFAeugtYsaV9w72nx:1nmHBUZMXojNPq/u7s+S274ItQ
MD5:	EB7FC93BB3263EEB66BA489D43CB51AD
SHA1:	B3A0BA916F954B0DA8AE7AC539303176757C0642
SHA-256:	520926A637841923CCE32BB1A6238FAF87C40CAA2C76269E05F42C05D47440CF
SHA-512:	96E789C2DF929CB4A656C630E7E99CCA9242930E1584EFF0EF56EDA9AE30FDBB975A9B198406866AD5A92C45274C9B087BB8CEC91A678BFABC21085094F4681
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.=.1.3.3.1.4.2.4.3.3.7.1.5.1.5.8.9.9.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.1.4.2.4.3.3.7.2.7.1.9.0.1.4.3.....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.=.b.2.0.e.a.6.5.e.-.3.6.2.c.-.4.6.b.3.-.b.3.6.9.-.3.3.c.c.1.4.1.d.9.6.8.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.3.e.4.9.b.a.4.-.c.5.9.b.-.4.8.b.8.-.8.6.b.e.-.9.d.8.4.f.f.7.5.9.7.1.3.....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...W.i.n.3.2...P.W.S.X.-.g.e.n...1.6.1.8.8...7.0.9.4...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.0.8.-.0.0.0.1.-.0.0.1.a.-.0.3.9.2.-.d.d.8.8.5.6.0.4.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.3.0.a.9.7.e.b.e.a.e.1.0.7.0.8.9.f.8.7.4.8.f.e.7.8.a.7.a.a.a.3.8.0.0.0.0.f.f.f.f.!.0.0.0.0.2.3.7.7.3.5.5.1.8.9.c.5.9.e.6.f.0.d.4.c.8.7.9.2.a.a.9.5.9.4.2.5.5.8.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Nov 30 00:56:12 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	40616
Entropy (8bit):	2.003000119461151
Encrypted:	false
SSDEEP:	192:ghhUkWXpDiOcgjV+T71PyznTM89xyc62DujPpIYtn:+6hcY+T7ZyzTN92PSCn
MD5:	3BCFE29C334432700B094F1FC88DD0F6
SHA1:	F9E2D5799A2FB03010AA8C16F46FEBF8F3C27E35
SHA-256:	3CCC35DB1139D794A77C61519F9A8BA09A7E97D3E054B8EE70BB1C089D482F7B
SHA-512:	71D099A9DAAA3DC006D4C225FF1DB28D99CD91A4F188CEAE81382F0644DBCAD0D0A4DE3C41AF371E566CF5D82B8908C7E53C83C24954387A6CCEBE7F816D0E3
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....,..c.....&.....T.....8.....T..... .....U.....B.....GenuineIntelW.....T.....)..c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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):	3.6979070914958747
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiFI6hXx5dv6YqASUMegmfIS0Cpr+89bx9UsfXzlm:RrlsNiq6hXx5dv6YNSUMegmfISbx9Hf0
MD5:	9A0987CA0C23DC8894104FD280D1C9CB
SHA1:	86A49E082370B17C4C9386B5008FB580BA8A221F
SHA-256:	4F9BF8E8B553A8DF0B80CBABBEB310193F14D9078FE513BC294342397ECC9F8A
SHA-512:	346E611884A82B1D470D45296F60A9BB7AE881CAE125D542E974A994B3CBB237CC79B3A5FAE9C54F36E2BADD51DF57EBBA60367B4394F962A84C72582437516B
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.>.5.6.4.0.</./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB55.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4787
Entropy (8bit):	4.559141635088195
Encrypted:	false
SSDEEP:	48:cvIwSD8zsFJgtWI9f3Wgc8sqYji8fm8M4JEwTZWaFlB+q81LG/tiE3P9zWz/d:ulTffwGgrsqYLJTB/nZ0/d
MD5:	955A54B626D1F0F1007DAAB9D2C55C57
SHA1:	9E2662E1C47A4A13C8D82BCB94D0395F91FEB409
SHA-256:	CDBCCAAC3A30A680FE826E60D0A549404F4161ECC925EEC1A1462371F4602A86
SHA-512:	AEF3C0DCBED91B7CEFE5ADF0B78FB7CC5075D9032BA452C27936693A929CA8D28B47F614A73D0CDFA6F71B41C246D94A9C95658FD5D87BCC6942ECBA7F61B36
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="1802046" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.182857922109804
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.Win32.PWSX-gen.16188.7094.exe
File size:	147968
MD5:	c852376dda1de89231d5f558255775e0
SHA1:	2377355189c59e6f0d4c8792aa959425585dbc61
SHA256:	2c9d6d1a184ed20ff0667797fe4d182170716fb1b179488979bc33f79a901208
SHA512:	35734b4b784630927e4da3cd2ffa69e664bdd0cedce1bfe7e8bc6f0c35b0f06174c05f553c4dd84b4843d257bc46892a9226ff6f719ff6fdcb06dd23fff8bb80
SSDEEP:	3072:8OPPLcLPR2kaQ+nYwZbBPUxRC/akBYcgVg7JkWmjwaY4YFOnJKwy:8iLcLPRi/xB8gFLm8oJKd
TLSH:	41E33B11B0C2C0B7C76724B301E796FB3A39B7219B615DDF5B580E686B395E0A630A37
File Content Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....c.....,.....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40d32c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x6385E3E9 [Tue Nov 29 10:50:17 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	8644442967ce2e1b40266fb36e00cd91

Entrypoint Preview
Instruction
call 00007F6A10CB93DBh
jmp 00007F6A10CB8FFFh
push ebp
mov ebp, esp
push dword ptr [ebp+08h]
call 00007F6A10CB918Fh
neg eax
pop ecx
sbb eax, eax
neg eax
dec eax
pop ebp
ret
push ebp
mov ebp, esp
cmp dword ptr [00425A60h], FFFFFFFFh
push dword ptr [ebp+08h]
jne 00007F6A10CB9189h
call 00007F6A10CBC612h
jmp 00007F6A10CB918Dh
push 00425A60h
call 00007F6A10CBC595h
pop ecx
neg eax
pop ecx
sbb eax, eax
not eax
and eax, dword ptr [ebp+08h]
pop ebp
ret
push 00000008h
push 00422EA8h
call 00007F6A10CB9701h
and dword ptr [ebp-04h], 00000000h
mov eax, 00005A4Dh
cmp word ptr [00400000h], ax
jne 00007F6A10CB91DFh
mov eax, dword ptr [0040003Ch]
cmp dword ptr [eax+00400000h], 00004550h
jne 00007F6A10CB91CEh
mov ecx, 0000010Bh
cmp word ptr [eax+00400018h], cx
jne 00007F6A10CB91C0h
mov eax, dword ptr [ebp+08h]

Instruction
mov ecx, 00400000h
sub eax, ecx
push eax
push ecx
call 00007F6A10CB9302h
pop ecx
pop ecx
test eax, eax
je 00007F6A10CB91A9h
cmp dword ptr [eax+24h], 00000000h
jl 00007F6A10CB91A3h
mov dword ptr [ebp-04h], FFFFFFFEh
mov al, 01h
jmp 00007F6A10CB91A1h
mov eax, dword ptr [ebp-14h]
mov eax, dword ptr [eax]
xor ecx, ecx
cmp dword ptr [eax], C0000005h
sete cl
mov eax, ecx
ret
mov esp, dword ptr [ebp-18h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x21788	0x118	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x29000	0x1a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2a000	0x14c4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x1c560	0xc0	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x21c1c	0x37c	.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	0x1a0d0	0x1a200	False	0.4765998803827751	data	6.254058720378555	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x1c000	0x7424	0x7600	False	0.4095272775423729	Matlab v4 mat-file (little endian) , numeric, rows 0, columns 4309148	4.9666568554916495	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x24000	0x258c	0xa00	False	0.16171875	data	2.098226797581286	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.00cfg	0x27000	0x8	0x200	False	0.03125	data	0.06116285224115448	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.voltbl	0x28000	0x22	0x200	False	0.091796875	data	0.6504699138522845	
.rsrc	0x29000	0x1a8	0x200	False	0.486328125	data	4.183569951400347	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x2a000	0x14c4	0x1600	False	0.7718394886363636	data	6.426785687436811	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x29060	0x143	XML 1.0 document, ASCII text	English	United States

Imports

DLL	Import
SHLWAPI.dll	GetMenuPosFromID, PathRemoveExtensionA, SHRegQueryUSValueW, StrRChrW, UrlEscapeA
ole32.dll	CreateClassMoniker, EnableHookObject, HMETAFILE_UserUnmarshal, OleInitialize, StgCreateStorageEx, WriteStringStream
MSWSOCK.dll	GetTypeByNameW, TransmitFile, getnetbyname
WINMM.dll	joyGetNumDevs, midiStreamPosition, midiStreamRestart, mixerClose, mixerGetLineControlsW
pdh.dll	PdhConnectMachineA, PdhGetDefaultPerfCounterA, PdhRemoveCounter, PdhVbGetCounterPathElements, PdhVbGetOneCounterPath, PdhVbOpenQuery
OLEAUT32.dll	OleLoadPictureEx, VARIANT_UserMarshal, VarDateFromCy, VarR8Pow, VarUI2FromDate
CRYPT32.dll	CertDuplicateStore, CertFindRDNAttr, CertFreeCertificateContext, CryptMsgCountersign
RPCRT4.dll	NdrByteCountPointerBufferSize, NdrClientInitializeNew, NdrUserMarshalUnmarshall, RpcBindingInqAuthInfoW, RpcBindingSetOption, RpcMgmtEnableIdleCleanup, RpcMgmtInqComTimeout
KERNEL32.dll	CloseHandle, CreateEventW, CreateFileW, CreateThread, DecodePointer, DeleteCriticalSection, EncodePointer, EnterCriticalSection, EnumSystemCodePagesW, ExitProcess, FindClose, FindFirstFileExW, FindNextFileW, FlushFileBuffers, FreeEnvironmentStringsW, FreeLibrary, GetACP, GetCPInfo, GetCommandLineA, GetCommandLineW, GetConsoleMode, GetConsoleOutputCP, GetCurrentProcess, GetCurrentProcessId, GetCurrentThreadId, GetEnvironmentStringsW, GetFileSize, GetFileType, GetLastError, GetModuleFileNameW, GetModuleHandleExW, GetModuleHandleW, GetOEMCP, GetProcAddress, GetProcessHeap, GetStartupInfoW, GetStdHandle, GetStringTypeW, GetSystemTimeAsFileTime, GlobalAlloc, GlobalLock, GlobalReAlloc, GlobalSize, GlobalUnlock, HeapAlloc, HeapFree, HeapReAlloc, HeapSize, InitializeCriticalSectionAndSpinCount, InitializeSListHead, IsDebuggerPresent, IsProcessorFeaturePresent, IsValidCodePage, LCMapStringW, LeaveCriticalSection, LoadLibraryExW, MulDiv, MultiByteToWideChar, QueryPerformanceCounter, RaiseException, ReadFile, RtlUnwind, SetFilePointerEx, SetLastError, SetStdHandle, SetUnhandledExceptionFilter, TerminateProcess, TlsAlloc, TlsFree, TlsGetValue, TlsSetValue, UnhandledExceptionFilter, VirtualAlloc, WaitForMultipleObjects, WideCharToMultiByte, WriteConsoleW, WriteFile, lstrcmpW, lstrcpyW, lstrlenW
USER32.dll	AdjustWindowRect, BeginPaint, CharLowerBuffW, CharUpperBuffW, ClientToScreen, CloseClipboard, CreateCaret, CreateMenu, CreatePopupMenu, CreateWindowExW, DefWindowProcW, DestroyCaret, DispatchMessageW, EmptyClipboard, EnableMenuItem, EndPaint, FillRect, GetCapture, GetClientRect, GetClipboardData, GetDC, GetDlgItem, GetDpiForSystem, GetFocus, GetKeyboardState, GetParent, GetSystemMenu, GetSystemMetrics, GetWindowLongW, HideCaret, InsertMenuW, InvalidateRect, InvertRect, IsClipboardFormatAvailable, IsWindowVisible, LoadCursorW, LoadIconW, LoadStringW, MapVirtualKeyW, MsgWaitForMultipleObjects, OpenClipboard, PeekMessageW, PostMessageW, PostQuitMessage, RegisterClassW, ReleaseCapture, ReleaseDC, ScrollWindow, SetCapture, SetCaretPos, SetClipboardData, SetRect, SetScrollPos, SetScrollRange, SetTimer, SetWindowLongW, SetWindowPos, SetWindowTextW, ShowCaret, ShowScrollBar, ShowWindow, SystemParametersInfoW, ToUnicode, TrackPopupMenu, UpdateWindow, VkKeyScanW, wsprintfW
GDI32.dll	BitBlt, CreateBitmap, CreateCompatibleBitmap, CreateCompatibleDC, CreateFontIndirectW, CreateSolidBrush, DeleteObject, EnumFontFamiliesExW, GetStockObject, GetTextFaceW, GetTextMetricsW, LineTo, MoveToEx, SelectObject, SetBkColor, SetTextColor, TextOutW, TranslateCharsetInfo
COMCTL32.dll	
ADVAPI32.dll	RegCloseKey, RegCreateKeyW, RegSetValueExW

Possible Origin

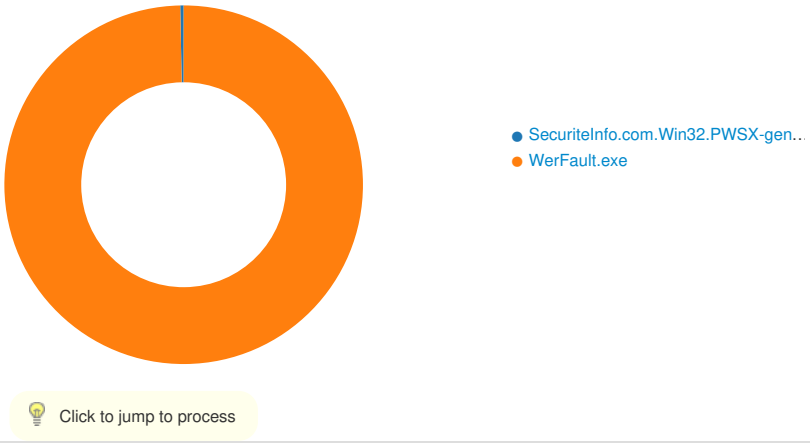
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Win32.PWSX-gen.16188.7094.exe PID: 5640, Parent PID: 3452

General

Target ID:	0
Start time:	16:56:09
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.16188.7094.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.PWSX-gen.16188.7094.exe
Imagebase:	0x1a0000
File size:	147968 bytes
MD5 hash:	C852376DDA1DE89231D5F558255775E0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
unknown	unknown	4294967295	object type mismatch	1	1A1A1D	ReadFile

Analysis Process: WerFault.exe PID: 5688, Parent PID: 5640

General

Target ID:	2
Start time:	16:56:10
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5640 -s 464
Imagebase:	0x2b0000

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	6D911717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB55.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB55.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_c136f9839aaccad85a66b9f733bbb3cf4c588e0_e9cd6a7e_166ff3ee	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_c136f9839aaccad85a66b9f733bbb3cf4c588e0_e9cd6a7e_166ff3ee\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D90497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB55.tmp	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB55.tmp.xml	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA40.tmp.csv	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA60.tmp.txt	success or wait	1	6D90497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 2c fd fd 63 fd 05 12 00 00 00 00 00	MDMP ,c	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	6052	6	00 00 00 00 00 00		success or wait	1	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.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 17 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 08 16 00 00 29 fd 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 0d 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)c0Pacific Standard TimePacific Daylight Time	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	7036	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 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 fd fd fd fd 00 fd 31 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 4f 00 26 1a 1a 00 23 00 00 00 02 02 01 00 08 fd 4f 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	+S++1O&#O+	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	1620	168	0c 16 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 26 1a 1a 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 fd 02 00 00 7c 1b 00 00	&|	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	9900	20	11 00 00 00 3c fd fd 77 00 00 00 00 00 01 00 00 fd 27 00 00	<w'	success or wait	17	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	10176	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	16	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	33284	256	1c fd 45 0b 45 fd 31 49 04 24 fd 44 24 04 00 00 00 00 fd 15 48 1d 1c 00 fd fd 08 fd 45 0b 45 fd 31 fd fd 04 24 00 00 00 00 fd 44 24 04 fd 44 24 08 00 30 00 00 fd 44 24 0c 40 00 00 00 fd 15 00 1e 1c 00 fd fd 10 fd 45 0b 4d 0b 55 0b 75 0d 45 fd 31 fd fd 34 24 fd 54 24 04 fd 4c 24 08 fd 44 24 0c fd 44 24 10 00 00 00 00 fd 15 fd 1d 1c 00 fd fd 14 fd 45 0b 4d fd 0f fd 14 08 fd fd 1d fd 14 08 fd 45 0b 4d fd fd 14 08 fd fd 01 fd 14 08 fd 45 0b 4d fd 0f fd 14 08 fd fd 17 fd 14 08 fd 45 0b 4d fd fd 14 08 fd fd fd fd 14 08 fd 45 0b 4d fd 0f fd 14 08 fd fd fd 00 00 00 fd 14 08 fd 45 0b 4d fd 0f fd 14 08 fd fd 71 fd 14 08 fd 45 0b 4d fd 0f fd 14 08 fd fd fd 00 00 00 fd 14 08 fd 45 0b 4d fd 0f fd 14 08 fd fd 0e fd 14 08 fd	EE1DHEE1DD$0D$@EMUuE14TLDD$EMEMEMEMEMEMqEMEM	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	7752	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 fd 4f 00 fd fd fd 77 23 00 00 00 16 02 00 00 fd fd 4f 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 fd fd	?+S++ Ow#O+	success or wait	3	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	1888	48	14 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 10 32 00 00 00 00 00 fd fd fd 00 00 00 00 00 40 08 00 00 fd 29 00 00 fd 02 00 00 fd 23 00 00	2@)#	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	1948	4	20 00 00 00		success or wait	32	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	6058	98	5c 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 57 00 69 00 6e 00 33 00 32 00 2e 00 50 00 57 00 53 00 58 00 2d 00 67 00 65 00 6e 00 2e 00 31 00 36 00 31 00 38 00 38 00 2e 00 37 00 30 00 39 00 34 00 2e 00 65 00 78 00 65 00 00 00	\SecuriteInfo.com.Win32.PWSX-gen.16188.7094.exe	success or wait	32	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	5300	752	00 00 61 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 64 1b 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 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 00 70 fd 02 00 00 00 00 00 30 23 03 00 00 00 00 70 49 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 52 77 03 00 00 00 00 00 fd 79 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 1b 00 00 00 00 00 6d 7e 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 5b fd 04 00 00 00 00	at`A!-adBB?#@AZbp0#pIRwym~@[	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	33540	7076	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	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE76B.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 0d 00 00 fd 07 00 00 05 00 00 00 14 01 00 00 fd 26 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 12 00 00 00 fd 00 00 15 00 00 00 fd 01 00 00 20 15 00 00 16 00 00 00 fd 00 00 00 0c 17 00 00	&T8T	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 36 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5640</Pid>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1002	138	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 57 00 69 00 6e 00 33 00 32 00 2e 00 50 00 57 00 53 00 58 00 2d 00 67 00 65 00 6e 00 2e 00 31 00 36 00 31 00 38 00 38 00 2e 00 37 00 30 00 39 00 34 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.Win32.PWSX-gen.16188.7094.exe</ImageName>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1140	4	0d 00 0a 00		success or wait	1	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1144	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1148	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1238	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1242	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1246	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 39 00 36 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2969</Uptime>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1288	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1292	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1296	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1378	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1382	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1386	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1438	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1442	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1446	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1490	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1494	2	09 00		success or wait	3	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1500	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 36 00 30 00 38 00 39 00 35 00 32 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>60895232</PeakVirtualSize>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1586	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1590	2	09 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1596	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 36 00 30 00 38 00 38 00 37 00 30 00 34 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>60887040</VirtualSize>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1666	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1670	2	09 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1676	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 37 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2732</PageFaultCount>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1750	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1754	2	09 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1760	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 30 00 34 00 35 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>10604544</PeakWorkingSetSize>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1858	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1862	2	09 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1868	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 30 00 34 00 35 00 34 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>10604544</WorkingSetSize>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1950	4	0d 00 0a 00		success or wait	1	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1954	2	09 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	1960	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 38 00 32 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>108256</QuotaPeakPagedPoolUsage>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2074	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2078	2	09 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2084	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 37 00 36 00 38 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>107688</QuotaPagedPoolUsage>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2182	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2186	2	09 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2192	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 39 00 39 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>49920</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2316	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2320	2	09 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2326	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 39 00 35 00 36 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>49568</QuotaNonPagedPoolUsage>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2434	4	0d 00 0a 00		success or wait	1	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2438	2	09 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2444	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 36 00 31 00 36 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5361664</PagefileUsage>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2520	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2524	2	09 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2530	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 36 00 39 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5369856</PeakPagefileUsage>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2622	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2626	2	09 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2632	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 36 00 31 00 36 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5361664</PrivateUsage>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2704	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2708	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2712	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2758	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2762	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2766	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2796	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2800	2	09 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2806	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	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2846	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2850	2	09 00		success or wait	4	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2858	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2888	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2892	2	09 00		success or wait	4	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2900	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2970	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2974	2	09 00		success or wait	4	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	2982	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3072	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3076	2	09 00		success or wait	4	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3084	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 37 00 36 00 30 00 32 00 34 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5760249</Uptime>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3132	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3136	2	09 00		success or wait	4	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3144	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3222	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3226	2	09 00		success or wait	4	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3234	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3286	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3290	2	09 00		success or wait	4	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3298	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3342	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3346	2	09 00		success or wait	5	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3356	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3460	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3548	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 36 00 34 00 30 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>56401</PageFaultCount>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3624	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3628	2	09 00		success or wait	5	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3638	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 34 00 30 00 39 00 35 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121409536</PeakWorkingSetSize>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3752	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 30 00 35 00 37 00 32 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>121057280</WorkingSetSize>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3836	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3840	2	09 00		success or wait	5	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3850	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 31 00 34 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>1114632</QuotaPeakPagedPoolUsage>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3966	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3970	2	09 00		success or wait	5	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	3980	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 35 00 36 00 39 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>1056920</QuotaPagedPoolUsage>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4080	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4084	2	09 00		success or wait	5	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4094	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 30 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>90184</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4218	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4222	2	09 00		success or wait	5	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4232	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 37 00 36 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>77624</QuotaNonPagedPoolUsage>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4340	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4344	2	09 00		success or wait	5	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4354	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 30 00 30 00 32 00 37 00 35 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>45002752</PagefileUsage>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4446	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 35 00 34 00 36 00 39 00 34 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>46546944</PeakPagefileUsage>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4540	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4544	2	09 00		success or wait	5	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4554	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 30 00 30 00 32 00 37 00 35 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>45002752</PrivateUsage>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4628	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4632	2	09 00		success or wait	4	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4640	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4686	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4690	2	09 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4696	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4738	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4742	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4746	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4778	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4782	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4784	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4826	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4830	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4832	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4870	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4874	2	09 00		success or wait	2	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4878	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4940	4	0d 00 0a 00		success or wait	8	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4944	2	09 00		success or wait	16	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	4948	142	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 57 00 69 00 6e 00 33 00 32 00 2e 00 50 00 57 00 53 00 58 00 2d 00 67 00 65 00 6e 00 2e 00 31 00 36 00 31 00 38 00 38 00 2e 00 37 00 30 00 39 00 34 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.Win32.PWSX-gen.16188.7094.exe</Parameter0>	success or wait	8	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	5680	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	5684	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	5686	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	5726	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	5730	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	5732	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	5770	4	0d 00 0a 00		success or wait	6	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	5774	2	09 00		success or wait	12	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	5778	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6332	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6336	2	09 00		success or wait	1	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6338	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6378	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6382	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6384	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6422	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6426	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6430	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6524	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6528	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6532	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 66 00 6c 00 67 00 77 00 66 00 64 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>flgwfd, Inc.</SystemManufacturer>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6638	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6642	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6646	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 66 00 6c 00 67 00 77 00 66 00 64 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>flgwfd7,1</SystemProductName>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6742	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6746	2	09 00		success or wait	2	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6750	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6870	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6874	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6878	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 33 00 34 00 34 00 35 00 36 00 37 00 32 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>1634456721</OSInstallDate>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6960	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6964	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	6968	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7070	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7074	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7078	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7146	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7150	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7152	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7192	4	0d 00 0a 00		success or wait	1	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7196	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7198	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7232	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7236	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7240	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7336	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7340	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7342	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7378	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7382	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7384	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7408	4	0d 00 0a 00		success or wait	3	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7412	2	09 00		success or wait	6	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7416	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7660	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7664	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7666	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7692	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7696	2	09 00		success or wait	1	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7698	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 31 00 31 00 2d 00 33 00 30 00 54 00 30 00 30 00 3a 00 35 00 36 00 3a 00 31 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-30T00:56:12Z">	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7798	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7802	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	7806	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 36 00 34 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 33 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 33 00 34 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="300" PID="5640" UptimeMS="234" TimeSinceCreationMS="234" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	8064	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	8068	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	8092	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	8096	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	8136	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	8140	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	8180	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	8184	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	8188	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 32 00 30 00 65 00 61 00 36 00 35 00 65 00 2d 00 33 00 36 00 32 00 63 00 2d 00 34 00 36 00 62 00 33 00 2d 00 62 00 33 00 36 00 39 00 2d 00 33 00 33 00 63 00 63 00 31 00 34 00 31 00 64 00 39 00 36 00 38 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>b20ea65e-362c-46b3-b369-33cc141d9680</Guid>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	8286	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	8290	2	09 00		success or wait	2	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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 32 00 2d 00 31 00 31 00 2d 00 33 00 30 00 54 00 30 00 30 00 3a 00 35 00 36 00 3a 00 31 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>2022-11-30T00:56:12Z</CreationTime>	success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	8392	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	8396	2	09 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.tmp.WERInternalMetadata.xml	8438	4	0d 00 0a 00		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA98.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	6D90497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB55.tmp.xml	0	4787	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	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_c136f9839aaccad85a66b9f733bbb3cf4c588e0_e9cd6a7e_166ff3ee\Report.wer	0	2	fd fd		success or wait	1	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_c136f9839aaccad85a66b9f733bbb3cf4c588e0_e9cd6a7e_166ff3ee\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	157	6D90497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_c136f9839aaccad85a66b9f733bbb3cf4c588e0_e9cd6a7e_166ff3ee\Report.wer	10802	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 39 00 31 00 33 00 35 00 30 00 37 00 36 00 39 00 39 00	MetadataHash=913507699	success or wait	1	6D90497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	success or wait	1	6D9236BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D921FB2	RegCreateKeyExW
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9043D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	ProgramId	unicode	000630a97ebeae107089f8748fe78a7aaa380000ffff	success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	FileId	unicode	00002377355189c59e6f0d4c8792aa959425585dbc61	success or wait	1	6D9236BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	LowerCaseLongPath	unicode	c:\users\user\desktop\securiteinfo.com.win32.pwsx-gen.16188.7094.exe	success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	LongPathHash	unicode	securiteinfo.com|cad89d86	success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	Name	unicode	securiteinfo.com.win32.pwsx-gen.16188.7094.exe	success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	Publisher	unicode		success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	Version	unicode		success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	BinFileVersion	unicode		success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	BinaryType	unicode	pe32_i386	success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	ProductName	unicode		success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	ProductVersion	unicode		success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	LinkDate	unicode	11/29/2022 10:50:17	success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	BinProductVersion	unicode		success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	Size	B	00 42 02 00 00 00 00 00	success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	Language	dword	0	success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	IsPeFile	dword	1	success or wait	1	6D9236BF	unknown
\REGISTRY\A\{efceb550-ce2d-c9ce-2fdc-03f454bdc669}\Root\InventoryApplicationFile\securiteinfo.com|cad89d86	IsOsComponent	dword	0	success or wait	1	6D9236BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 26 1A 1A 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	6D921FE8	RegSetValueExW

Disassembly

No disassembly