ID: 800793
Sample Name:
SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe
Cookbook: default.jbs
Time: 19:54:11
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

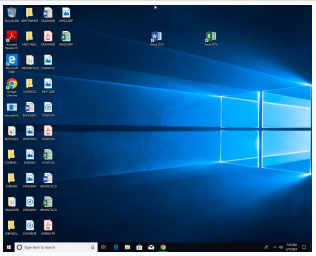
Windows Analysis Report

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

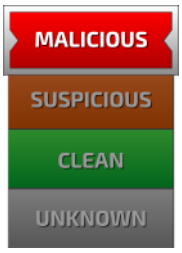
Overview

General Information

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



Detection

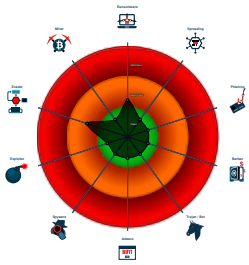


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe (PID: 5380 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe MD5: BD13975ABC6AC3E5A97706A45F48F7DF)
  - WerFault.exe (PID: 5168 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5380 -s 212 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 4732 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5380 -s 212 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

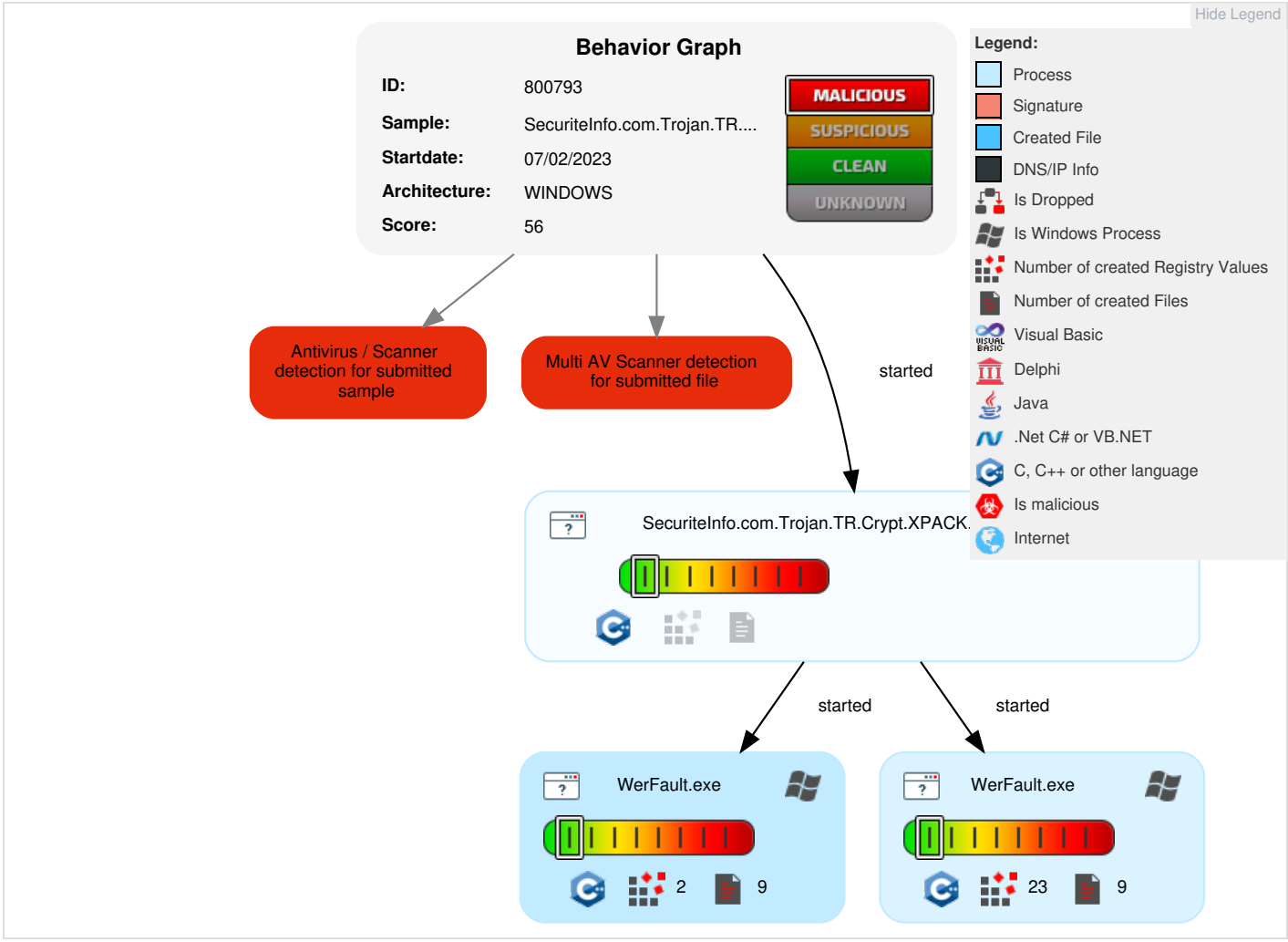
Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Virtualization/Sandbox Evasion	OS Credential Dumping	2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe	13%	ReversingLabs		
SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe	13%	Virustotal		Browse
SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe	100%	Avira	TR/Crypt.XPACK.Gen	

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.clamav.net	SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe	false		high
http://upx.sf.net	Amcache.hve.2.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800793
Start date and time:	2023-02-07 19:54:11 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe
Detection:	MAL
Classification:	mal56.winEXE@3/10@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 23%) • Quality average: 19.5% • Quality standard deviation: 36.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): WerFault.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.22

- Excluded domains from analysis (whitelisted): fs.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus17.westus.cloudapp.azure.com, watson.telemetry.microsoft.com

Simulations

Behavior and APIs

Time	Type	Description
19:55:12	API Interceptor	2x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_7a157073226634c33dd8e08437f6e586c2306e78_5c1322d7_140d63f1\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):	0.6808475373763749
Encrypted:	false
SSDEEP:	384:JuwL9H2YbKBUZMX/FOjE/u7slX4lt6lG:JKBUiljE/u7slX4lt
MD5:	675DF585318392F90EEEBFFA74772394
SHA1:	51DD951A3470B87215241561A225937885205A8D
SHA-256:	C98CEE238826F8AF47B0534AC9D8DBEB4DAC59372892D5EED01B8FD7A95B5E72
SHA-512:	6C5A85018B8E66FA34FEDACF5A981B4FAA575A5F3100DE08FF9E44E8711DA3D6FD3DA9DFF03762D64F47E81D0D332D406CF4090A1AAEFA4994D9E02F34FAF4BC
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.2.0.3.0.2.1.0.9.9.4.5.4.1.5.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.0.3.0.2.1.1.0.3.8.2.9.2.4.8.....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.=.2.f.3.3.7.e.2.8.-.b.8.5.e.-.4.c.7.6.-.b.5.e.1.-.a.e.9.2.6.4.9.1.0.3.5.a.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.4.3.0.6.b.5.4.-.5.e.c.8.-.4.7.8.c.-.9.c.9.9.-.2.7.f.d.4.6.3.8.f.3.5.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...T.R...C.r.y.p.t...X.P.A.C.K...G.e.n...2.3.8.6.2...2.3.7.8.8...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.0.4.-.0.0.0.1.-.0.0.1.a.-.b.2.6.e.-.2.9.2.3.7.1.3.b.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.6.e.4.4.4.f.b.3.6.6.f.a.4.3.2.4.0.c.d.5.7.5.d.7.a.5.8.e.1.3.b.3.0.0.0.0.f.f.f.f.!.0.0.0.0.1.5.4.e.7.0.c.5.1.5.0.8.1.5.3.0.8.e.1.7.b.b.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_f8b2f5d487f13ef078ee9e48b4dedc7a1e0c36a_5c1322d7_12416ae6\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):	0.6882862139900008
Encrypted:	false
SSDEEP:	192:dUbos19H2Y4yOHK5SGFOjE/u7slS274lt6IG:QL9H2Y4yGK5SGFOjE/u7slX4lt6IG
MD5:	5C802FDC9258D4C422B908E1A9199C17
SHA1:	BB55D6311C953C3780CA6D3DB3A2BA7C1359AE6D
SHA-256:	E0E30358BA3145A62EFE32279CD39E22F1421A32E12B6CB09FBD84A5D026A371
SHA-512:	81584731E1DED48C7EFCCA20A4DB5E35107C1FAB567A8014EEB12371E2601D28B94F74A03210471751681B5680053FF7F3D20309E604208B7C1165C20FC51246
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.2.0.3.0.2.1.1.2.8.7.1.0.5.4.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.0.3.0.2.1.1.3.1.6.7.9.3.1.7.....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.=.e.b.3.2.2.8.8.b.-.a.2.2.0.-.4.9.3.0.-.9.f.e.c.-.d.c.9.e.8.2.a.f.0.a.c.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.c.0.1.6.a.b.8.-.e.b.c.c.-.4.f.6.0.-.b.1.5.5.-.2.6.6.b.d.5.7.7.9.0.7.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...T.r.o.j.a.n...T.R...C.r.y.p.t...X.P.A.C.K...G.e.n...2.3.8.6.2...2.3.7.8.8...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.0.4.-.0.0.0.1.-.0.0.1.a.-.b.2.6.e.-.2.9.2.3.7.1.3.b.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.6.e.4.4.4.f.b.3.6.6.f.a.4.3.2.4.0.c.d.5.7.5.d.7.a.5.8.e.1.3.b.3.0.0.0.0.f.f.f.f.!.0.0.0.0.1.5.4.e.7.0.c.5.1.5.0.8.1.5.3.0.8.e.1.7.b.b.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 8 03:55:10 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	18136
Entropy (8bit):	2.2140371705131296
Encrypted:	false
SSDEEP:	96:5Zt8ie8Q/JU3aVWrii7kVVtIIzrLz6RaDMQ3Zq/X7hIWIXYWIPI4MSsYsDx:n2imJU3liOWIInnu8MQ3oh9MhYsDx
MD5:	BF4EB60248C867C56419DF9CF7657519
SHA1:	DE9FEA3810F0DBBEBEB800858C156055E2879E0E
SHA-256:	5560C9B7FEE8C5A21A17DD24A19C2C60E2E6A8E058725741E30C7815C7D87FA5
SHA-512:	FDAB7CA66CA29F0736649FD342DF8FA405EB95AC0794F61E590A7FDF515FC00865993D4F197EDF73C459812A149683B4D86A63ED2EA8A5C75E13546D14D739F
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....c.....4..... ...<.....T..I.....T.....8.....T.....>.....\.....H.....U.....B.....GenuineIntelW.....T.....c.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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):	8486
Entropy (8bit):	3.710326506184381
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWljJ6KE6YqrSUW2gmf9V9SvoCprO89bJpsfa5jm:RrlsNiWZJ6KE6Y2SUW2gmf9vSfJCfaA
MD5:	F5872CD21339B5167D64893B6615A69A
SHA1:	446C4979569D6C1130469DA17DB58B372669DF0F
SHA-256:	E2CA09FC8563A54AD902CFE041FC853BBAB2A94D556452B6F7E63F78D49A2327
SHA-512:	592E77832D9D36203C7C953E2226376D0498A0FC7865E83559BC363DEDC89581B239D5F4367B7A826F3FB06636F351ADE5034B1BA9AD258BAA054E981F97571D
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.>.5.3.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF4.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4827
Entropy (8bit):	4.6160992504504925
Encrypted:	false
SSDEEP:	48:cvIwSD8zsKJgtWI9G5whWgc8sqYjA8fm8M4JKJvZFV+q8+5vqtU1+xzd:uITfYNZgrsqYxJOJJqtU1+xzd
MD5:	9E81828FD2871BD58BF9158C9E5DDF55
SHA1:	BFF1598ED8D194B5606151C59665B82707CC3E2A
SHA-256:	2A9A356CAC9D09D89002B4E043893D1512E0E5B2CF37868F212CE598D5B86812
SHA-512:	9B7F85D0A488D2CB8E9726F1E1046573A3F6E95D42E4538F79EE7DFDA911EF03CDD9258906EAEF60D97A9B453870B425077BEF7F186A28D6B771DD924F37CC34
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="1903025" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 8 03:55:12 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	18004
Entropy (8bit):	2.1905200670195244
Encrypted:	false
SSDEEP:	96:5jt8if8Q/JMtby0Lrzii7kqLFBx30z6RaDMQ3Zq/X7tbIWIXYWIPIwK0dCqM:l2izJMt203ziO3BQu8MQ3otblSqM
MD5:	B5AD25738C307412F601597EBC0BAEC7
SHA1:	D7B8605663D59AAF2DF30F06C820161175DA7A7C
SHA-256:	49199EA201FF47045D33CF42E1651F798B03B07C3324B61DC6B4F73FD2EF7C4E
SHA-512:	8B2C5D03D36438BE7DFEC596A4D299C893A824DCAD02B630158B4A32ACB4D48581F9F5283D389D4BD7336906D13C18A7C2CFD6B6D07332B7A42E36101F0FFF4
Malicious:	false
Reputation:	low
Preview:	MDMP..... ....c.....4..... ...<.....D...l.....T.....8.....T.....=.....\.....H.....U.....B.....GenuineIntelW.....T.....c.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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):	8592
Entropy (8bit):	3.718620236587172
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWlQ6Rj6YqESUV4gmf9VYXS8oCpDI89bypsf1VGm:RrlsNiWy6Rj6YJSUV4gmf9mXSEyCfn
MD5:	EC026D8D95F395B4B65DA67067C041CB
SHA1:	6507B2D5B4A699493DB326FC07AF52F58F18C1B1
SHA-256:	161AFBB00DD82146A0CA7795A4120571AA634932FA5B7124A87B201D5DD3FD7C
SHA-512:	EF677AE8B58BD2DD5A008A834CE7CB4B6BBF89D288E5982F34A21521B8CB97E7F3F1F70BD6A1A1E66046A771573A509BEF41A4F4F7A2D4C2CB66649EFA86B153
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.3.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6700.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4925
Entropy (8bit):	4.668748771547563
Encrypted:	false
SSDEEP:	48:cvIwSD8zsKJgtWI9G5whWgc8sqYjcS8fm8M4JK+PFzz+q81PotU1+xzd:uITfYNZgrsqYsJbDtU1+xzd
MD5:	9F4B9FDF6B7BE719D8BD5C2192338737
SHA1:	E17855DEB6567014FBFF397EE05DF557A6B76A01
SHA-256:	FC4E67B491C2A4975A782F57326FF33F69B8500F02B20A73A8DD2E54FB8B9D4E
SHA-512:	9DE07F6A72D6BF0990888CD024B04729F250F2DB2421C5FC42C86C9B68B1061AA6A04FF1A4933F26F1002C94D3620E4AE49841DF0A3C2EA6DA7A1CA55D7F971E
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1903025" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.294366692569002
Encrypted:	false
SSDEEP:	12288:bnhAPB36rum3nMdyU1FWmlONYCdEA+Xepp5vl7Gaj+bOEKLibALvyRGS:LhAPB36rumXMdylwmliy
MD5:	766626AB7E88251178A3C5B7B8E3D940
SHA1:	E5DDD4E403F0CE02265D1A5C979FE6649A8C0F1D
SHA-256:	F67B9496AA9F1CE6AB25A6CBBC6C308DA6D858324877B2B97F04F026B37C7C16
SHA-512:	1FE94E211B6F61CE591730C5571B766C1871E4AA5C9CDDD8340971DDA413C7C6ADD97AF0B2DCD84D0A56D0E824213F0ED22C3E369B9C5EC58D6D57EDFED8499
Malicious:	false
Preview:	regf^...^...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmj.a#q;..... .....[\h~..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.754839213094983
Encrypted:	false
SSDEEP:	384:JY5/+nll4BA+CD6rIYn88/TVgGka+kODvkZH1BLw9n:J+/+nll0A+TD887VgGDWDvALw9
MD5:	19923D9CF7DF46214C99F515BE08FB05
SHA1:	708B4339B41C7E29BBA1D692C5445EB3D2290C37
SHA-256:	B6983A52522C17E10CEA28663F2648E94178F0259F4793C7BADFF96EDEC368D4
SHA-512:	1FC5E1C7FC76715D87B441347DB542E8DD59C77E854AAA92812D6F99237680ADAB4C98C9A7DCB2FA6DB0580610B46D5A171D26F1A0151D1848E5BCA4FFE5081
Malicious:	false
Preview:	regf]...]...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmj.a#q;..... .....]\h~HvLE.^.....].....%.....~..... ..hbin.....p.\.,.....nk,..fc#q;..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..fc#q;..... ....Z.....Root.....lf.....Root....nk ..fc#q;.....}..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck...

Static File Info

General

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

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

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

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 004234E8h
push 0041CA40h
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
sub esp, 58h
push ebx
push esi
push edi

Instruction
mov dword ptr [ebp-18h], esp
call dword ptr [004230CCh]
xor edx, edx
mov dl, ah
mov dword ptr [0042C508h], edx
mov ecx, eax
and ecx, 000000FFh
mov dword ptr [0042C504h], ecx
shl ecx, 08h
add ecx, edx
mov dword ptr [0042C500h], ecx
shr eax, 10h
mov dword ptr [0042C4FCh], eax
push 00000001h
call 00007F5FD2688346h
pop ecx
test eax, eax
jne 00007F6000C2823Ah
push 0000001Ch
call 00007F5F95388346h
pop ecx
call 00007F6078908346h
test eax, eax
jne 00007F6000C2823Ah
push 00000010h
call 00007F5F95388346h
pop ecx
xor esi, esi
mov dword ptr [ebp-04h], esi
call 00007F5FC7158346h
call dword ptr [004230C8h]
mov dword ptr [0042CB34h], eax
call 00007F60468F8346h
mov dword ptr [0042C560h], eax
call 00007F5FF98C8346h
call 00007F60408C8346h
call 00007F5F88128346h
mov dword ptr [ebp-30h], esi
lea eax, dword ptr [ebp-5Ch]
push eax
call dword ptr [00423088h]
call 00007F5FE88B8346h
mov dword ptr [ebp-64h], eax
test byte ptr [ebp-30h], 00000001h
je 00007F6000C28238h
movzx eax, word ptr [ebp+00h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x23f88	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x23000	0x1a8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

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

Network Behavior

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

Statistics

Behavior

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe PID: **5380**, Parent PID: **3452**

General

Target ID:	0
Start time:	19:55:09
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe
Imagebase:	0x400000
File size:	188416 bytes
MD5 hash:	BD13975ABC6AC3E5A97706A45F48F7DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: **5168**, Parent PID: **5380**

General

Target ID:	2
Start time:	19:55:09
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5380 -s 212
Imagebase:	0x8f0000
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	6CED1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF4.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_7a157073226634c33dd8e08437f6e586c2306e78_5c1322d7_140d63f1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_7a157073226634c33dd8e08437f6e586c2306e78_5c1322d7_140d63f1\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CEC497A	unknown

File Deleted				
File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF4.tmp	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF4.tmp.xml	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD5F.tmp.csv	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD7F.tmp.txt	success or wait	1	6CEC497A	unknown

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 1e 1d fd 63 fd 05 12 00 00 00 00 00	MDMP c	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	3040	6	00 00 00 00 00 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 0b 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 04 15 00 00 1d 1d fd 63 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 01 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	UBGenuineIntelWTc02Pacific Standard TimePacific Daylight Time	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	3284	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 6b fd 41 00 6b fd 41 00 00 60 3f 00 6b fd 41 00 6b fd 41 00 fd fd 19 00 fd fd 19 00 00 00 00 00 23 00 00 00 16 02 01 00 08 fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++kAkA`?kAkA#+	success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	1620	168	fd 15 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 0c 00 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	4716	20	05 00 00 00 00 60 3f 00 00 00 00 00 fd 04 00 00 fd 12 00 00	`?	success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	4800	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 fd 0a 69 00 00 00 00 00 00 00 69 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 01 00 01 00 00 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 01 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@{wiiyw{w0(Pm `fwPSwB	success or wait	4	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	10332	4212	fd fd fd 77 fd 1a 54 77 fd fd fd fd fd fd 19 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 00 00 00 fd 00 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 60 3f 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wTw$`?	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	1788	4	01 00 00 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	4000	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 6b fd 41 00 6b fd 41 00 00 00 00 00 20 fd 19 00 fd fd fd 77 23 00 00 00 16 02 00 00 fd fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++kAkA w#+	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	1792	48	fd 15 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 3f 00 00 00 00 00 fd fd 19 00 00 00 00 00 74 10 00 00 5c 28 00 00 fd 02 00 00 fd 0f 00 00	?t\(	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	1852	4	05 00 00 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	3046	122	74 00 00 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 54 00 52 00 2e 00 43 00 72 00 79 00 70 00 74 00 2e 00 58 00 50 00 41 00 43 00 4b 00 2e 00 47 00 65 00 6e 00 2e 00 32 00 33 00 38 00 36 00 32 00 2e 00 32 00 33 00 37 00 38 00 38 00 2e 00 65 00 78 00 65 00 00 00	tSecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe	success or wait	5	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	2288	752	00 00 fd 73 00 00 00 00 00 fd 09 00 fd fd 09 00 51 fd 0f fd fd 0c 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 30 fd 02 00 00 00 00 00 30 23 03 00 00 00 00 fd 7b 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 72 fd 03 00 00 00 00 00 3b 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 76 1b 00 00 00 00 00 70 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 5b fd 04 00 00 00 00	sQBB?$@AZb00#{rvp@[	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	14544	3592	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5A9A.tmp.dmp	32	108	03 00 00 00 34 00 00 00 fd 06 00 00 04 00 00 00 20 02 00 00 3c 07 00 00 05 00 00 00 54 00 00 00 6c 12 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 08 00 00 08 3e 00 00 15 00 00 00 fd 01 00 00 5c 09 00 00 16 00 00 00 fd 00 00 00 48 0b 00 00	4 <TIT8T>\H	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 33 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5380</Pid>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1002	162	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 54 00 52 00 2e 00 43 00 72 00 79 00 70 00 74 00 2e 00 58 00 50 00 41 00 43 00 4b 00 2e 00 47 00 65 00 6e 00 2e 00 32 00 33 00 38 00 36 00 32 00 2e 00 32 00 33 00 37 00 38 00 38 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe</ImageName>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1164	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1168	2	09 00		success or wait	2	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1172	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1262	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1266	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1270	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 35 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1055</Uptime>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1320	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1402	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1406	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1410	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1462	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1466	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1470	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1514	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1518	2	09 00		success or wait	3	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1524	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 37 00 30 00 39 00 32 00 36 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>170926 08</PeakVirtualSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1610	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1614	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1620	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 31 00 33 00 31 00 37 00 37 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>13131776</ VirtualSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1690	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1694	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1700	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 38 00 32 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>829</ PageFaultCount>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1772	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1776	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1782	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 30 00 34 00 37 00 34 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3 047424</P eakWorkingSetSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1878	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1882	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1888	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 30 00 34 00 37 00 34 00 32 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>30474 24</WorkingSetSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1968	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1972	2	09 00		success or wait	3	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	1978	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 32 00 34 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>32432</QuotaPeakPagedPoolUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2090	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2094	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2100	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 35 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>24520</QuotaPagedPoolUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2196	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2200	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2206	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 30 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>8056</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2328	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2332	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2338	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>7784</QuotaNonPagedPoolUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2444	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2448	2	09 00		success or wait	3	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2454	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>573440</PagefileUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2528	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2532	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2538	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 31 00 36 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>581632</PeakPagefileUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2628	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2632	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2638	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>573440</PrivateUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2708	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2712	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2716	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2762	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2766	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2770	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2810	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2850	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2854	2	09 00		success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2862	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2904	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2974	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2978	2	09 00		success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	2986	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3088	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 30 00 31 00 39 00 36 00 37 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4019675</Uptime>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3136	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3140	2	09 00		success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3148	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3226	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3230	2	09 00		success or wait	4	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3238	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3302	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3346	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3350	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3360	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3450	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3454	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3464	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3538	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3542	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3552	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 37 00 34 00 31 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>57413</PageFaultCount>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3628	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3632	2	09 00		success or wait	5	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3642	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 30 00 39 00 30 00 39 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>120909824</PeakWorkingSetSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3742	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3746	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3756	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 30 00 38 00 34 00 38 00 33 00 38 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>120848384</WorkingSetSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3840	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3844	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3854	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 31 00 38 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>1118632</QuotaPeakPagedPoolUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3970	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3974	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	3984	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 35 00 39 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1065968</QuotaPagedPoolUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4084	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4088	2	09 00		success or wait	5	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4098	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4222	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4226	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4236	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 37 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>77760</QuotaNonPagedPoolUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4344	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4348	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4358	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 31 00 30 00 31 00 30 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>45101056</PagefileUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4436	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4440	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4450	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 38 00 37 00 34 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>46874624</PeakPagefileUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4544	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4548	2	09 00		success or wait	5	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4558	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 31 00 30 00 31 00 30 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>45101056</PrivateUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4632	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4636	2	09 00		success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4690	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4694	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4700	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4742	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4746	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4750	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4782	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4786	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4788	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4830	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4834	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4836	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4874	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4878	2	09 00		success or wait	2	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4882	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4944	4	0d 00 0a 00		success or wait	8	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4948	2	09 00		success or wait	16	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	4952	166	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 54 00 52 00 2e 00 43 00 72 00 79 00 70 00 74 00 2e 00 58 00 50 00 41 00 43 00 4b 00 2e 00 47 00 65 00 6e 00 2e 00 32 00 33 00 38 00 36 00 32 00 2e 00 32 00 33 00 37 00 38 00 38 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe</Parameter0>	success or wait	8	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	5684	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	5688	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	5690	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	5730	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	5734	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	5736	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	5774	4	0d 00 0a 00		success or wait	6	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	5778	2	09 00		success or wait	12	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	5782	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6336	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6340	2	09 00		success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6342	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6382	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6386	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6388	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6426	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6430	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6434	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6528	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6532	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6536	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 6c 00 6a 00 75 00 6e 00 79 00 69 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>ljunyi, Inc.</SystemManufacturer>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6642	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6646	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6650	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6a 00 75 00 6e 00 79 00 69 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>ljunyi7,1</SystemProductName>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6746	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6750	2	09 00		success or wait	2	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6754	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6874	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6878	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6882	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 32 00 36 00 33 00 30 00 37 00 36 00 31 00 37 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>1626307617</OSInstallDate>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6964	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6968	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	6972	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7074	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7078	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7082	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7150	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7154	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7156	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7196	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7200	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7202	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7236	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7240	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7244	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7340	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7344	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7346	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7382	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7386	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7388	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7412	4	0d 00 0a 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7416	2	09 00		success or wait	6	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7420	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7664	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7668	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7670	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7696	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7700	2	09 00		success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7702	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 32 00 2d 00 30 00 38 00 54 00 30 00 33 00 3a 00 35 00 35 00 3a 00 31 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-02-08T03:55:10Z">	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7802	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7806	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	7810	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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 33 00 38 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="304" PID="5380" UptimeMS="109" TimeSinceCreationMS="109" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8068	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8072	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8076	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8096	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8100	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8102	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8140	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8144	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8146	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	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8184	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8188	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8192	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 66 00 33 00 33 00 37 00 65 00 32 00 38 00 2d 00 62 00 38 00 35 00 65 00 2d 00 34 00 63 00 37 00 36 00 2d 00 62 00 35 00 65 00 31 00 2d 00 61 00 65 00 39 00 32 00 36 00 34 00 39 00 31 00 30 00 33 00 35 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>2f337e28-b85e-4c76-b5e1-ae926491035a</Guid>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8290	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8294	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8298	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 32 00 2d 00 30 00 38 00 54 00 30 00 33 00 3a 00 35 00 35 00 3a 00 31 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-02-08T03:55:10Z</CreationTime>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8396	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8400	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8402	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8442	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B57.tmp.WERInternalMetadata.xml	8446	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	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5BF4.tmp.xml	0	4827	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_7a157073226634c33dd8e08437f6e586c2306e78_5c1322d7_140d63f1\Report.wer	0	2	fd fd		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_7a157073226634c33dd8e08437f6e586c2306e78_5c1322d7_140d63f1\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	130	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_7a157073226634c33dd8e08437f6e586c2306e78_5c1322d7_140d63f1\Report.wer	8102	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 30 00 32 00 33 00 32 00 37 00 39 00 37 00 37 00 34 00	MetadataHash=-1023279774	success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	success or wait	1	6CEE36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6CEE1FB2	RegCreateKeyExW
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CEC43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	ProgramId	unicode	00066e444fb366fa43240cd575d7a58e13b30000ffff	success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	FileId	unicode	0000154e70c5150815308e17bbb74cae4ee79948e438	success or wait	1	6CEE36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	LowerCaseLongPath	unicode	c:\users\user\desktop\securiteinfo.com.trojan.tr.crypt.xpack.gen.23862.23788.exe	success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	LongPathHash	unicode	securiteinfo.com|f47bdf91	success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	Name	unicode	securiteinfo.com.trojan.tr.crypt.xpack.gen.23862.23788.exe	success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	Publisher	unicode		success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	Version	unicode		success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	BinFileVersion	unicode		success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	BinaryType	unicode	pe32_i386	success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	ProductName	unicode		success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	ProductVersion	unicode		success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	LinkDate	unicode	01/27/2011 10:43:15	success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	BinProductVersion	unicode		success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	Size	B	00 E0 02 00 00 00 00 00	success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	Language	dword	0	success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	IsPeFile	dword	1	success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\securiteinfo.com|f47bdf91	IsOsComponent	dword	0	success or wait	1	6CEE36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CEE1FE8	RegSetValueExW

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

Analysis Process: WerFault.exe PID: **4732**, Parent PID: **5380**

General

Target ID:	4
Start time:	19:55:12
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5380 -s 212
Imagebase:	0x8f0000
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	6CED1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6700.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6700.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_f8b2f5d487f13ef078ee9e48b4dedc7a1e0c36a_5c1322d7_12416ae6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_f8b2f5d487f13ef078ee9e48b4dedc7a1e0c36a_5c1322d7_12416ae6\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CEC497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6700.tmp	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6700.tmp.xml	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD86D.tmp.csv	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD87E.tmp.txt	success or wait	1	6CEC497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 20 1d fd 63 fd 05 12 00 00 00 00 00	MDMP c	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	3040	6	00 00 00 00 00 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 0b 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 04 15 00 00 1d 1d fd 63 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 01 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 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	UBGenuineIntelWTc02Pacific Standard TimePacific Daylight Time	success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	3284	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 70 fd 19 00 fd fd fd 77 40 fd 41 00 78 fd 19 00 fd fd 19 00 fd fd fd fd 23 00 00 00 02 02 01 00 7c fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++pw@Ax#|+	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	1620	168	fd 15 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 0c 00 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	4716	20	04 00 00 00 00 60 3f 00 00 00 00 00 fd 04 00 00 fd 12 00 00	`?	success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	4784	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 fd 0a 69 00 00 00 00 00 00 00 69 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 01 00 01 00 00 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 01 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@{wiiyw{w0(Pm `fwPSwB	success or wait	3	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	10060	4488	00 00 00 00 fd fd 41 00 70 fd 19 00 fd fd fd fd fd 19 00 fd fd 19 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 19 00 52 fd fd 77 78 fd 19 00 70 fd 19 00 fd fd 19 00 24 fd 19 00 70 fd 19 00 fd fd fd 77 70 fd 19 00 fd fd 19 00 24 fd fd 77 78 fd 19 00 70 fd 19 00 fd fd 19 00 24 fd 19 00 40 fd 41 00 78 fd 19 00 fd fd 19 00 70 fd 19 00 51 21 fd 77 78 fd 19 00 70 fd 19 00 fd fd 19 00 24 fd 19 00 40 fd 41 00 fd fd fd fd 00 00 00 00 fd fd 19 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ApRwxppwpwxp$@AxpQ!wxp$@A	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	1788	4	01 00 00 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	4000	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 70 fd 19 00 fd fd fd 77 40 fd 41 00 78 fd 19 00 fd fd 19 00 fd fd fd fd 23 00 00 00 02 02 01 00 7c fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++pw@Ax#|+	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	1792	48	fd 15 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 3f 00 00 00 00 00 78 fd 19 00 00 00 00 00 fd 11 00 00 4c 27 00 00 fd 02 00 00 fd 0f 00 00	?xL'	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	1852	4	05 00 00 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	3046	122	74 00 00 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 54 00 52 00 2e 00 43 00 72 00 79 00 70 00 74 00 2e 00 58 00 50 00 41 00 43 00 4b 00 2e 00 47 00 65 00 6e 00 2e 00 32 00 33 00 38 00 36 00 32 00 2e 00 32 00 33 00 37 00 38 00 38 00 2e 00 65 00 78 00 65 00 00 00	tSecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe	success or wait	5	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	2288	752	00 00 fd 73 00 00 00 00 00 fd 09 00 fd fd 09 00 51 fd 0f fd fd 0c 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd 02 00 00 00 00 00 30 23 03 00 00 00 00 11 7d 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 49 03 00 00 00 00 00 3b 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 74 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 5b fd 04 00 00 00 00	sQBB?$@AZb0#}t@[	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	14548	3456	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6604.tmp.dmp	32	108	03 00 00 00 34 00 00 00 fd 06 00 00 04 00 00 00 20 02 00 00 3c 07 00 00 05 00 00 00 44 00 00 00 6c 12 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 08 00 00 fd 3d 00 00 15 00 00 00 fd 01 00 00 5c 09 00 00 16 00 00 00 fd 00 00 00 48 0b 00 00	4 <DIT8T=\H	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 33 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5380</Pid>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1002	162	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 54 00 52 00 2e 00 43 00 72 00 79 00 70 00 74 00 2e 00 58 00 50 00 41 00 43 00 4b 00 2e 00 47 00 65 00 6e 00 2e 00 32 00 33 00 38 00 36 00 32 00 2e 00 32 00 33 00 37 00 38 00 38 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe</ImageName>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1164	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1168	2	09 00		success or wait	2	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1172	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1262	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1266	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1270	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 38 00 38 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>3887</Uptime>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1320	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1402	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1406	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1410	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1462	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1466	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1470	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1514	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1518	2	09 00		success or wait	3	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1524	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 37 00 30 00 39 00 32 00 36 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>17092608</PeakVirtualSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1610	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1614	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1620	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 31 00 32 00 37 00 36 00 38 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>13127680</VirtualSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1690	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1694	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1700	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 38 00 33 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>833</PageFaultCount>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1772	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1776	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1782	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 30 00 35 00 39 00 37 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3059712</PeakWorkingSetSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1878	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1882	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1888	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 30 00 35 00 35 00 36 00 31 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3055616</WorkingSetSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1968	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1972	2	09 00		success or wait	3	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	1978	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 32 00 34 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>32432</QuotaPeakPagedPoolUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2090	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2094	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2100	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 35 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>24512</QuotaPagedPoolUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2196	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2200	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2206	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 31 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>9160</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2328	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2332	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2338	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 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>9024</QuotaNonPagedPoolUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2444	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2448	2	09 00		success or wait	3	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2454	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>573440</PagefileUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2528	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2532	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2538	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 31 00 36 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>581632</PeakPagefileUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2628	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2632	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2638	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>573440</PrivateUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2708	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2712	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2716	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2762	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2766	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2770	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2810	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2850	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2854	2	09 00		success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2862	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2904	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2974	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2978	2	09 00		success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	2986	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3088	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 30 00 32 00 32 00 35 00 30 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4022506</Uptime>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3136	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3140	2	09 00		success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3148	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3226	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3230	2	09 00		success or wait	4	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3238	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3302	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3346	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3350	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3360	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3450	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3454	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3464	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3538	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3542	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3552	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 37 00 39 00 33 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>57935</PageFaultCount>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3628	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3632	2	09 00		success or wait	5	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3642	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 31 00 36 00 31 00 38 00 34 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121618432</PeakWorkingSetSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3742	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3746	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3756	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 31 00 32 00 34 00 39 00 37 00 39 00 32 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>121249792</WorkingSetSize>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3840	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3844	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3854	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 31 00 38 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>1118632</QuotaPeakPagedPoolUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3970	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3974	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	3984	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 36 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1066664</QuotaPagedPoolUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4084	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4088	2	09 00		success or wait	5	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4098	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4222	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4226	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4236	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 38 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>77896</QuotaNonPagedPoolUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4344	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4348	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4358	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 31 00 37 00 38 00 38 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>45178880</PagefileUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4436	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4440	2	09 00		success or wait	5	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4450	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 38 00 37 00 34 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>46874624</PeakPagefileUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4544	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4548	2	09 00		success or wait	5	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4558	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 31 00 37 00 38 00 38 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>45178880</PrivateUsage>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4632	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4636	2	09 00		success or wait	4	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4690	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4694	2	09 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4700	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4742	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4746	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4750	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4782	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4786	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4788	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4830	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4834	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4836	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4874	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4878	2	09 00		success or wait	2	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4882	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4944	4	0d 00 0a 00		success or wait	8	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4948	2	09 00		success or wait	16	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	4952	166	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 54 00 52 00 2e 00 43 00 72 00 79 00 70 00 74 00 2e 00 58 00 50 00 41 00 43 00 4b 00 2e 00 47 00 65 00 6e 00 2e 00 32 00 33 00 38 00 36 00 32 00 2e 00 32 00 33 00 37 00 38 00 38 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>SecuriteInfo.com.Trojan.TR.Crypt.XPACK.Gen.23862.23788.exe</Parameter0>	success or wait	8	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	5782	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	5786	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	5788	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	5828	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	5832	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	5834	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	5872	4	0d 00 0a 00		success or wait	6	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	5876	2	09 00		success or wait	12	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	5880	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6434	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6438	2	09 00		success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6440	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6480	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6484	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6486	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6524	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6528	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6532	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6626	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6630	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6634	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 6c 00 6a 00 75 00 6e 00 79 00 69 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>ljunyi, Inc.</SystemManufacturer>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6740	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6744	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6748	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 6c 00 6a 00 75 00 6e 00 79 00 69 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>ljunyi7,1</SystemProductName>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6844	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6848	2	09 00		success or wait	2	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6852	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6972	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6976	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	6980	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 32 00 36 00 33 00 30 00 37 00 36 00 31 00 37 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>1626307617</OSInstallDate>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7062	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7066	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7070	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7180	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7248	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7252	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7254	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7294	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7298	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7300	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7334	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7338	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7342	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7438	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7442	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7444	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7480	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7484	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7486	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7510	4	0d 00 0a 00		success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7514	2	09 00		success or wait	6	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7518	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>80000000</Flags>	success or wait	3	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7770	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7774	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7776	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7802	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7806	2	09 00		success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7808	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 32 00 2d 00 30 00 38 00 54 00 30 00 33 00 3a 00 35 00 35 00 3a 00 31 00 33 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-02-08T03:55:13Z">	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7908	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7912	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	7916	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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 33 00 38 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="304" PID="5380" UptimeMS="109" TimeSinceCreationMS="109" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8174	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8178	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8182	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8202	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8206	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8208	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8246	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8250	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8252	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	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8290	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8294	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8298	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 62 00 33 00 32 00 32 00 38 00 38 00 62 00 2d 00 61 00 32 00 32 00 30 00 2d 00 34 00 39 00 33 00 30 00 2d 00 39 00 66 00 65 00 63 00 2d 00 64 00 63 00 39 00 65 00 38 00 32 00 61 00 66 00 30 00 61 00 63 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>eb32288b-a220-4930-9fec-dc9e82af0ac8</Guid>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8396	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8400	2	09 00		success or wait	2	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8404	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 32 00 2d 00 30 00 38 00 54 00 30 00 33 00 3a 00 35 00 35 00 3a 00 31 00 33 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-02-08T03:55:13Z</CreationTime>	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8502	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8506	2	09 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8508	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	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8548	4	0d 00 0a 00		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A1.tmp.WERInternalMetadata.xml	8552	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	6CEC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6700.tmp.xml	0	4925	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_f8b2f5d487f13ef078ee9e48b4dedc7a1e0c36a_5c1322d7_12416ae6\Report.wer	0	2	fd fd		success or wait	1	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_f8b2f5d487f13ef078ee9e48b4dedc7a1e0c36a_5c1322d7_12416ae6\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	130	6CEC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_f8b2f5d487f13ef078ee9e48b4dedc7a1e0c36a_5c1322d7_12416ae6\Report.wer	8202	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 33 00 37 00 35 00 31 00 32 00 38 00 39 00 31 00 30 00	MetadataHash=-375128910	success or wait	1	6CEC497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CEE36BF	unknown
\REGISTRY\A\{3a52133f-bb59-6ced-5f1e-641ef122b3e2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CEC43D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 FD CB FA 86 02 00 00 00 00 00 00 00 FD CB FA 86 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CEE1FE8	RegSetValueExW

Disassembly

No disassembly