ID: 800788
Sample Name:
SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe
Cookbook: default.jbs
Time: 19:46:54
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

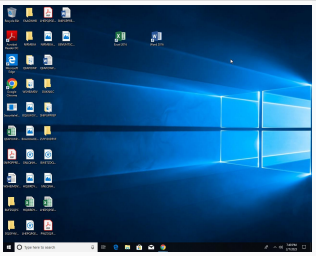
Windows Analysis Report

SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe

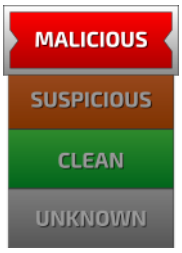
Overview

General Information

Sample Name:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe
Analysis ID:	800788
MD5:	d0adfd6a3ae38..
SHA1:	6ebe1f86e07fb...
SHA256:	1e7586126018...
Tags:	exe
Infos:	



Detection

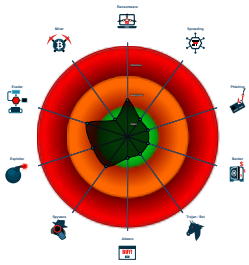


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub...
- Multi AV Scanner detection for subm...
- Machine Learning detection for sam...
- Creates a DirectInput object (often f...
- Uses 32bit PE files
- AV process strings found (often use...
- Found inlined nop instructions (likely...
- PE file does not import any functions
- One or more processes crash
- Uses code obfuscation techniques (...
- Checks if the current process is bei...
- PE file contains sections with non-s...

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe (PID: 2368 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe MD5: D0ADFD6A3AE38491118D11E6CAACD186)
  - WerFault.exe (PID: 2328 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2368 -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

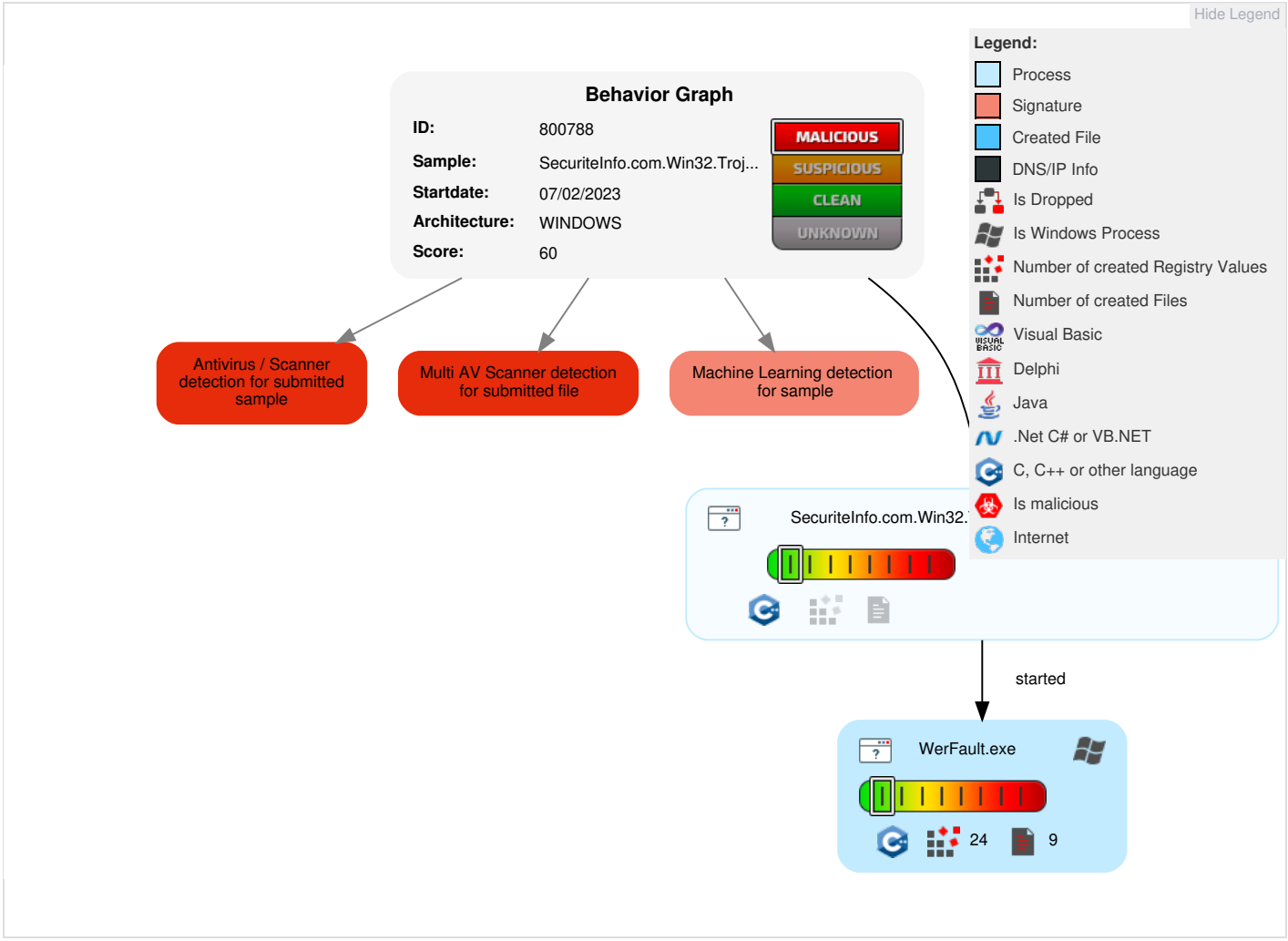
Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	1 Process Injection	1 Virtualization/Sandbox Evasion	1 Input Capture	2 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 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

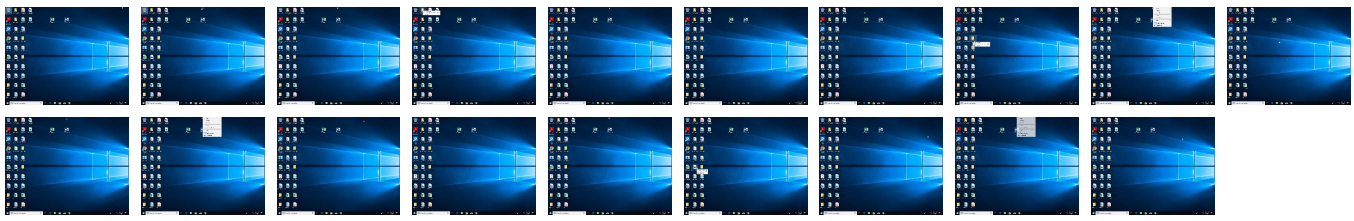
Behavior Graph



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.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	38%	ReversingLabs		
SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	31%	Virustotal		Browse
SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	100%	Avira	TR/Crypt.XPACK.Gen	
SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://5bcfae2f38d0e143c888d07ec9733d8c.s	0%	Avira URL Cloud	safe	
http://https://usher.ttvnw.net:	0%	Avira URL Cloud	safe	
http://https://bd4a0c7567edeaa0401463857c28ead7.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://eaassets-a.akam	0%	Avira URL Cloud	safe	
http://https://c58c9f027b8d0739f6b6d94b831e1010.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://usher.ttvnw.net:	0%	Virustotal		Browse
http://https://104.16.52.111	0%	Avira URL Cloud	safe	
http://https://aa88a8ab3fabc0c5d90ca85c9442a948.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://95df2ea9aba3e1cad7f8f4526047b63b.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://5a895ed07aed1b254ee21cd78958ae0b.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://steamcommunity-a.akamaihd.ne	0%	Avira URL Cloud	safe	
http://https://link.twitch.	0%	Avira URL Cloud	safe	
http://https://c2491d9d37e95faee1c67e314ae9a4bb.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://104.16.54.111	0%	Avira URL Cloud	safe	
http://https://2f16aa2ed3889461cd1076540300a6b3.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://6d7b94f6a3142075c6e14f949daff580.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://104.17.2.37	0%	Avira URL Cloud	safe	
http://https://gql.twitc	0%	Avira URL Cloud	safe	
http://https://06b67885560f95cbdf0ba34722e8d33c.steam302.xyz	0%	Avira URL Cloud	safe	
http://usher.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://1da58962a7dd53edd9775f6f74ff14e5.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://162.159.129.233	0%	Avira URL Cloud	safe	
http://https://162.159.129.232	0%	Avira URL Cloud	safe	
http://https://gateway.discord.gg:	0%	Avira URL Cloud	safe	
http://https://2973c6ca0e111662ed293b57dbae9fbf.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://6d859be7aa0440f65c8a940ef5218337.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://steamcommunity-a.akam	0%	Avira URL Cloud	safe	
http://https://2f9e9e61f7236db30c1ce0bb9d53581b.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://steamcommunity-a.akamai	0%	Avira URL Cloud	safe	
http://https://104.16.51.111	0%	Avira URL Cloud	safe	
http://https://7106a273bf3bbce901b765718ecbe69b.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://b3a0f6b6d20e3408d1725780186c54d3.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://890c88446f94f25bd32a3f1e0df6c120.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://fb96613da2b5475079b93f4be2e94cd3.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://gateway.discord.gg	0%	Avira URL Cloud	safe	
http://https://eaassets-a.akamaihd	0%	Avira URL Cloud	safe	
http://https://43658a3dbcfbc284a9030abbc3691c30.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://dbc180c27b3635f9e5b006f3a037b87e.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://e320c9db4f90dd219ab379f6a5e50dbd.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://104.16.53.111	0%	Avira URL Cloud	safe	
http://https://steampipe.ak	0%	Avira URL Cloud	safe	
http://https://104.16.55.111	0%	Avira URL Cloud	safe	
http://https://985a89155dd090eacda1b82388e334ed.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://5dd1e18eb1a29671b73c32e518b37111.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://e8304b1598fbfa673d2055f0a3342d7a.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://91b1eb7256ac2992f03fe0c7e7ef998d.steam302.xyz	0%	Avira URL Cloud	safe	
http://https://1d23669ea58a590fd66d9204d4301563.steam302.xyz	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://images-ext-1.discordapp.net:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://5bcfae2f38d0e143c888d07ec9733d8c.s	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://www.dogfight360.com/blog	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://countess.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://eaassets-a.akam	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://c58c9f027b8d0739f6b6d94b831e1010.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://cvp.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://status.discordapp.com:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://dev.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://passport.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://bd4a0c7567edeaa0401463857c28ead7.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://gds-vhs-drops-campaign-images.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://id-cdn.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://usher.ttvnw.net:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://104.16.52.111	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://aa88a8ab3fabc0c5d90ca85c9442a948.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://discordapp.com:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://steamuserimages-a.akamaihd.net	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://95df2ea9aba3e1cad7f8f4526047b63b.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://5a895ed07aed1b254ee21cd78958ae0b.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://c2491d9d37e95faee1c67e314ae9a4bb.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://vod-metro.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://api.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://www.clamav.net	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://origin-a.akamaihd.net:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://steamcommunity-a.akamaihd.ne	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://link.twitch.	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://id.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://link.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://eaassets-a.akamaihd.net	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://104.16.54.111	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://clips.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aws.amazon.com	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://104.17.2.37	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://2f16aa2ed3889461cd1076540300a6b3.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://pubsub-edge.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://6d7b94f6a3142075c6e14f949daff580.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://gql.twitc	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://06b67885560f95cbdf0ba34722e8d33c.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://us-west-2.uploads-regional.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://steamcn.com/t419530-1-1	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://1da58962a7dd53edd9775f6f74ff14e5.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://dl.discordapp.net:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://usher.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://steamcdn-a.akamaihd.net:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://music.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://steamstore-a.akamaihd.net	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://player.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://www.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://162.159.129.233	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://162.159.129.232	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://clips-media-assets2.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://m.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://gateway.discord.gg:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://2973c6ca0e111662ed293b57dbae9fbf.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://6d859be7aa0440f65c8a940ef5218337.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://gateway.discord.gg	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://images-ext-2.discordapp.net:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://vod-storyboards.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://vluki-a.akamaihd.net	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://steamcommunity-a.akam	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://irc-ws.chat.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://2f9e9e61f7236db30c1ce0bb9d53581b.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://app.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://steamcommunity-a.akamai	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://104.16.51.111	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://7106a273bf3bbce901b765718ecbe69b.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://platform.twitter.com:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://890c88446f94f25bd32a3f1e0df6c120.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://blog.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://b3a0f6b6d20e3408d1725780186c54d3.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://gql.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://extension-files.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://eaassets-a.akamaihd	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://fb96613da2b5475079b93f4be2e94cd3.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://43658a3dbcfbc284a9030abbc3691c30.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://client-event-reporter.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://104.16.53.111	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://inspector.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://cctv4-lh.akamaihd.net	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://e320c9db4f90dd219ab379f6a5e50dbd.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://dbc180c27b3635f9e5b006f3a037b87e.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://static2.cdn.ubi.com	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://steampipe.ak	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://toots-a.akamaihd.net	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://spade.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://media.discordapp.net:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://hgtv-i.akamaihd.net	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://support.discordapp.com:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://trowel.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://985a89155dd090eacda1b82388e334ed.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://store.steampowered.com:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://https://104.16.55.111	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://help.twitch.tv:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false		high
http://upx.sf.net	Amcache.hve.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://5dd1e18eb1a29671b73c32e518b37111.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://91b1eb7256ac2992f03fe0c7e7ef998d.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://e8304b1598fbfa673d2055f0a3342d7a.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown
http://https://1d23669ea58a590fd66d9204d4301563.steam302.xyz	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800788
Start date and time:	2023-02-07 19:46:54 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 46s
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe
Detection:	MAL
Classification:	mal60.winEXE@2/6@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 12.4% • Quality standard deviation: 15.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 13.89.179.12
- Excluded domains from analysis (whitelisted): fs.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, ctldl.windowsupdate.com, watson.telemetry.microsoft.com, onedsblobprdcus17.centralus.cloudapp.azure.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
19:48:02	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_8b8aab2d3044b37bde8ae2665b0819910cdd8be_73356 85e_095836a8\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):	0.6771188638551645
Encrypted:	false
SSDEEP:	96:VoFnPWV+zyQer9hMyoI7Jf/pXIQcQvc6QcEDMcw3DOWz+HbHg6ZAXGng5FMTPSkH:udo3ZHBUZMXAjE/u7sTS274Itk
MD5:	855206006F7DEE78BCE1AEA6CAD5982E
SHA1:	819FAAAB152AC17DEE80D375E9C7B3AECB15D878
SHA-256:	6E3344F79D2ACD5523E32711D9EECDCF4E3BC4D15FAC65BB9F90DDB7D4D292A6
SHA-512:	9A6602885CBAB2D09F5A0EF3D4D39B1B097DB970F2C05B6788C182ACD7C2B75B4187629B47BB637A73556A00235C3AEED42B92AEADA9215EB55342058D5DE6D8
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.=.1.3.3.2.0.3.0.1.6.7.4.1.1.2.5.8.3.6.....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.=.1.3.3.2.0.3.0.1.6.7.4.6.2.8.1.9.1.9.....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.b.8.e.b.5.4.4.-.7.a.0.7.-.4.2.9.0.-.b.f.e.2.-.7.2.e.4.b.6.3.2.5.d.8.6.....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.=.e.7.7.1.f.8.e.0.-.6.2.5.b.-.4.1.2.5.-.9.9.9.2.-.e.d.4.3.b.2.e.0.a.8.a.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...W.i.n.3.2...T.r.o.j.a.n...P.S.E...1.G.8.0.G.6.X...7.2.1.6...1.5.0.7.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.9.4.0.-.0.0.0.1.-.0.0.1.f.-.3.9.3.8.-.1.1.1.f.7.0.3.b.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.9.4.7.8.2.b.f.d.1.f.a.1.4.2.1.4.7.4.1.a.3.d.a.c.5.8.7.c.3.e.c.9.0.0.0.0.f.f.f.f.!.0.0.0.0.6.e.b.e.1.f.8.6.e.0.7.f.b.3.f.b.c.7.9.e.5.1.8.b.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 8 03:47:54 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	18032

Entropy (8bit):	2.1922587903575153
Encrypted:	false
SSDEEP:	96:5F8i48Q/Nbv7vvk/oi7knzlXzdSWMZS5JizwsyVe3WInWIX4I4uVIZa6G:AiM1DvsAOWdSWDbsyUwuVGnG
MD5:	AE621C78C119E91FC27977FD52858EAB
SHA1:	80086FC7E8599F7B90316C6927CA465015DFB714
SHA-256:	2121254F7BE9044CDF106E8BFFEEBB78E650919FA10A4C085F4FA35D4C6D5E8B
SHA-512:	6D387EFAE5C72E5EF96AA039C8018D7753C70B1F5DB0338A206C0138606B2CCC72198B95C22E1EE08B427B01F469E9509CAB791551BA200C6840D014AA8929B
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....j..c.....4..... ...<.....d...h.....T.....8.....T.....=.....\.....H.....U.....B.....GenuineIntelW.....T.....@...h..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\WER17F6.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):	8480
Entropy (8bit):	3.7105401924660883
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiSd60QwoIP6Yq5SUEy1gmf0MS+Cprj89bissf42m:RrlsNiI60QlP6YESUn1gmfHSii/fw
MD5:	70256A99F1DD8CBE33B9CE8F02AD6EEE
SHA1:	E20F8414A11357B3CB7D0578634508BDF83014FE
SHA-256:	CFF841143B8D66CE50B3D473DDCA12C8F37A761FD8FBF6E8E4DC0D9486896C37
SHA-512:	1127DDC2B7DBDECE4E4B3987499B684602ECCBC22E25D6DE0471004A3C9D105D5F80E7419648F90BDAD9DF4E8CA95345F64EC872033A9F9EC61C1A90A6E6908
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.>.2.3.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1864.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4813
Entropy (8bit):	4.602194128745111
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6JgtWI93nj7Wgc8sqYj18fm8M4JO2ZFBU+q8tm0zR+Nfd:uITflunjKgrsqYOJ9tUTAR+Nfd
MD5:	35C2E153841B86E09B989B4768A096C5
SHA1:	E19118841CFBB1A6212E6C1E6AF8B6CD26B528A6
SHA-256:	A2BCB5F5262B99458F405976AED5C4473470EB313895199C99111E1B96665BE6
SHA-512:	8A05A252E2964B5848B7B818EA0849D4C9BE0E14D993BD32620D0A1628A2CEAB70325355E950876ADF4FCDD81455FDD289CF9466847F9BB504D4D31B2E645BE2
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="1903018" />.. <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):	4.290622696417638
Encrypted:	false
SSDEEP:	12288:EJh78rBX4yWceTfEhlCThx3oQKikNn2uetWVzF16HkTWlsVdd55lqKo:S78rBX4yWceTfE0nc
MD5:	9E47AC22D77BC441C069E1E2C2C4623C
SHA1:	397EA6F12E1162D9AA4E40FFAC8402B6DC6681AE
SHA-256:	B1292BCD55E4F41DE36CDD321C17DDDC8E9C33F172E28832E92B34CD9E020626
SHA-512:	5B68E0F0633B76BF9CD0883F59734BB0EF9580ECE06CA9DC8A19D14069B838402A1A59D33601C37782304DD03311E2A42A9E1368942119D27052E924322590FD
Malicious:	false
Reputation:	low
Preview:	regfj...j...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.DR.p;..... .....[B..... .....

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):	28672
Entropy (8bit):	3.8182749306146797
Encrypted:	false
SSDEEP:	768:20DRftx1oJ4J3HNAJfAqpGpjkqIoSC9O4MYrWoE:hGWnTW
MD5:	4AC3F5994E3E77991C767220F1110171
SHA1:	A016E8F7BFD3E94F49C37CEEFA507A21CDD21E69
SHA-256:	B3A39D9A7FD3DAFA6802F4001BE77449DDECD4BFB4F5A364B4ED039E11D0A37D
SHA-512:	57E1707C2C43DC692F7EB69E13B20C29046EAE251E1BF1515811BA9882BAEB306465B8DA9692891B003E80BA7B35168144191CACC70EB01ED13B1D664824CB1 1
Malicious:	false
Preview:	regfi...i...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.DR.p;..... .....[BHvLE.n.....i.....-.../...tB.....0.....0..hbin.....p.\..,.....nk,.$.T.p;..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .$.T.p;..... ....Z.....Root.....lf.....Root....nk .$.T.p;.....}..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
Entropy (8bit):	5.690323528890668
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe
File size:	1221632
MD5:	d0adfd6a3ae38491118d11e6caacd186
SHA1:	6ebe1f86e07fb3fbc79e518bc6d8eb02913b11e1
SHA256:	1e7586126018ff22f443a86f027af1e94cb7746d0acdd4814c4970fe33d82b04
SHA512:	7ad4b2265159e6438cc8602430691029e700a7dbb8e476bafc3312fca4f3b1dfe42dee1b99ebb7bbbbe97f67e46a43250c5d20766e3b505cd0163caf74aa6daa
SSDEEP:	24576:8HrUZK3kA2VJT8TwnQCSPRI23bkmb5tSdaqOQgn9MX2R2XB4kVyigqlSiAClS9oD:84lIE9o9GjBraKQ1
TLSH:	0545AE72F78208E1D3101678C9FF2339DEB877960A25CD6B6694DD741E7A130BE26392
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.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48b8c3
Entrypoint Section:	.clam01
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, BYTES_REVERSED_LO, 32BIT_MACHINE, DEBUG_STRIPPED, REMOVABLE_RUN_FROM_SWAP, NET_RUN_FROM_SWAP, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x4D414C43 [Thu Jan 27 10:43:15 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	1
OS Version Minor:	0
File Version Major:	1
File Version Minor:	0
Subsystem Version Major:	1
Subsystem Version Minor:	0
Import Hash:	

Entrypoint Preview

Instruction
call 00007FF711FAAFD3h
jmp 00007FF7118B16D3h
mov eax, 00493234h
mov dword ptr [004E45F0h], eax
mov dword ptr [004E45F4h], 0049292Ah
mov dword ptr [004E45F8h], 004928DEh
mov dword ptr [004E45FCh], 00492917h
mov dword ptr [004E4600h], 00492880h
mov dword ptr [004E4604h], eax
mov dword ptr [004E4608h], 004931ACh
mov dword ptr [004E460Ch], 0049289Ch
mov dword ptr [004E4610h], 004927FEh
mov dword ptr [004E4614h], 0049278Ah
ret
mov edi, edi
push ebp
mov ebp, esp
call 00007FF7118C8DD3h
cmp dword ptr [ebp+08h], 00000000h
je 00007FF708E3C5B7h
call 00007FF712063AD3h
fnclex
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
cmp dword ptr [00509CC8h], 00000000h
je 00007FF708E3C63Dh

Instruction
sub esp, 08h
stmxcsr dword ptr [esp+04h]
mov eax, dword ptr [esp+04h]
and eax, 00007F80h
cmp eax, 00001F80h
jne 00007FF708E3C5C1h
fstcw word ptr [esp]
mov ax, word ptr [esp]
and ax, 007Fh
cmp ax, 007Fh
lea esp, dword ptr [esp+08h]
jne 00007FF708E3C60Ch

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	
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	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.clam01	0x1000	0xb1000	0xb1000	False	0.4473925229519774	data	6.649028182656562	IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_LNK_INFO, IMAGE_SCN_LNK_OVER, IMAGE_SCN_LNK_REMOVE, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_GPREL, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_MEM_SYSHEAP, IMAGE_SCN_MEM_PURGEABLE, IMAGE_SCN_MEM_16BIT, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_MEM_PRELOAD, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_128BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_LNK_NRELOC_OVFL, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_NOT_CACHED, IMAGE_SCN_MEM_NOT_PAGED, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.clam02	0xb2000	0x24000	0x24000	False	0.3477376302083333	data	5.185351349669696	IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_LNK_INFO, IMAGE_SCN_LNK_OVER, IMAGE_SCN_LNK_REMOVE, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_GPREL, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_MEM_SYSHEAP, IMAGE_SCN_MEM_PURGEABLE, IMAGE_SCN_MEM_16BIT, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_MEM_PRELOAD, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_128BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_LNK_NRELOC_OVFL, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_NOT_CACHED, IMAGE_SCN_MEM_NOT_PAGED, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.clam03	0xd6000	0x35000	0x35000	False	0.10202774911556604	data	2.060003423850223	IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_LNK_INFO, IMAGE_SCN_LNK_OVER, IMAGE_SCN_LNK_REMOVE, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_GPREL, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_MEM_SYSHEAP, IMAGE_SCN_MEM_PURGEABLE, IMAGE_SCN_MEM_16BIT, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_MEM_PRELOAD, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_128BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_LNK_NRELOC_OVFL, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_NOT_CACHED, IMAGE_SCN_MEM_NOT_PAGED, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.clam04	0x10b000	0xc000	0xc000	False	0.0074462890625	data	0.06664922320641793	IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_LNK_INFO, IMAGE_SCN_LNK_OVER, IMAGE_SCN_LNK_REMOVE, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_GPREL, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_MEM_SYSHEAP, IMAGE_SCN_MEM_PURGEABLE, IMAGE_SCN_MEM_16BIT, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_MEM_PRELOAD, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_128BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_LNK_NRELOC_OVFL, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_NOT_CACHED, IMAGE_SCN_MEM_NOT_PAGED, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

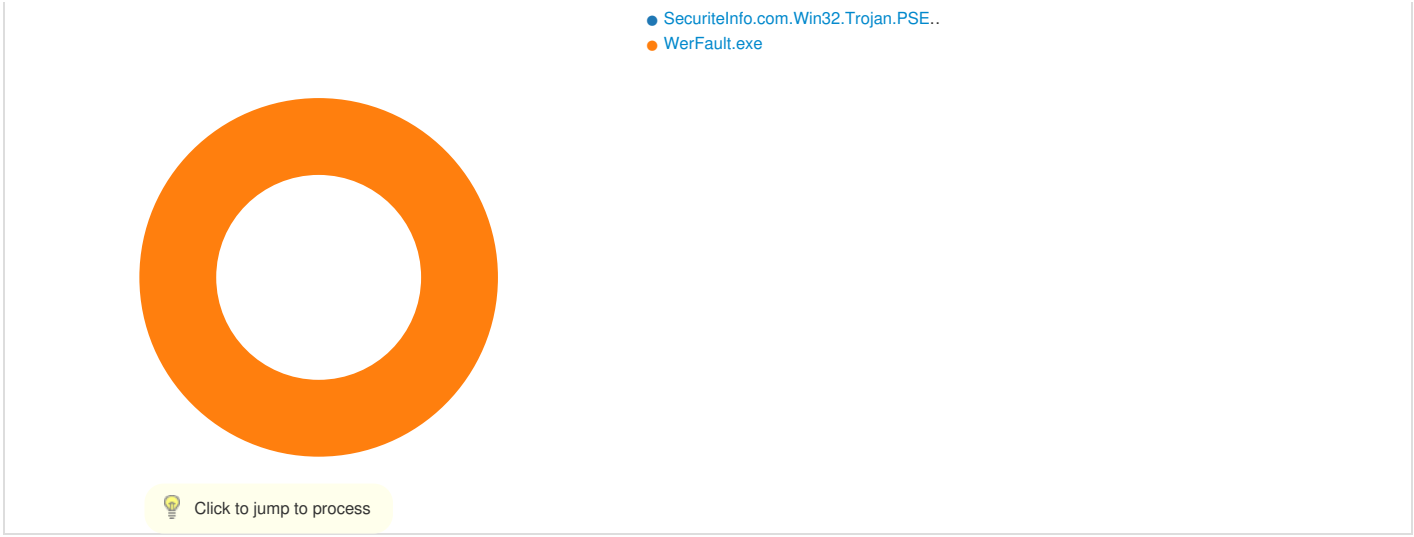
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.clam05	0x117000	0x14000	0x14000	False	0.29237060546875	data	3.9663953584370155	IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_LNK_INFO, IMAGE_SCN_LNK_OVER, IMAGE_SCN_LNK_REMOVE, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_GPREL, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_MEM_SYSHEAP, IMAGE_SCN_MEM_PURGEABLE, IMAGE_SCN_MEM_16BIT, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_MEM_PRELOAD, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_128BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_LNK_NRELOC_OVFL, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_NOT_CACHED, IMAGE_SCN_MEM_NOT_PAGED, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_EXECUTE, 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.Win32.Trojan.PSE.1G80G6X.7216.15072.exe PID: 2368, Parent PID: 3452

General	
Target ID:	0
Start time:	19:47:52
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe
Imagebase:	0x400000
File size:	1221632 bytes
MD5 hash:	D0ADFD6A3AE38491118D11E6CAACD186
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: 2328, Parent PID: 2368

General	
Target ID:	2
Start time:	19:47:53
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2368 -s 212
Imagebase:	0x340000
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	6C9E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1864.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1864.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_8b8aab2d3044b37bde8ae2665b0819910cdd8be_7335685e_095836a8	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_8b8aab2d3044b37bde8ae2665b0819910cdd8be_7335685e_095836a8\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C9D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1864.tmp	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1864.tmp.xml	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD9B3.tmp.csv	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD9F3.tmp.txt	success or wait	1	6C9D497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 6a 1b fd 63 fd 05 12 00 00 00 00 00	MDMP jc	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	3040	6	00 00 00 00 00 00		success or wait	1	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.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 54 05 00 00 fd 03 00 00 40 09 00 00 68 1b 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	UBGenuineIntelWT@hc02Pacific Standard TimePacific Daylight Time	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	3280	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 f8 48 00 f8 48 00 00 20 2c 00 f8 48 00 f8 48 00 49 5b fd 5b fd fd 19 00 fd 5f 09 23 00 00 00 46 02 01 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++HH ,HHI[[_#F+	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	1620	168	fd 07 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 5f 09 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 5f 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	4712	20	06 00 00 00 00 20 2c 00 00 00 00 00 fd 04 00 00 fd 12 00 00	,	success or wait	6	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	4812	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 fd 17 fd 00 00 00 00 00 00 00 fd 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 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 03 00 00 00 0a 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 00 00 00 00 00	@{wyw{w0(Pm `fwPSwB	success or wait	5	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	10348	4092	fd fd fd 77 fd 1a fd 76 fd fd fd fd 38 fd 19 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 00 00 00 fd 00 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 20 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 38 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 00 00 00 00 00 00 00 00	wv8$,8	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	1788	4	01 00 00 00		success or wait	1	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	3996	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 f8 48 00 f8 48 00 00 00 00 00 fd fd 19 00 fd fd fd 77 23 00 00 00 02 02 00 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	?+S++HHw#+	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	1792	48	fd 07 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 50 2c 00 00 00 00 00 04 fd 19 00 00 00 00 00 fd 0f 00 00 6c 28 00 00 fd 02 00 00 fd 0f 00 00	P,l(	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	1852	4	05 00 00 00		success or wait	5	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	3046	118	70 00 00 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 57 00 69 00 6e 00 33 00 32 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 50 00 53 00 45 00 2e 00 31 00 47 00 38 00 30 00 47 00 36 00 58 00 2e 00 37 00 32 00 31 00 36 00 2e 00 31 00 35 00 30 00 37 00 32 00 2e 00 65 00 78 00 65 00 00 00	pSecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe	success or wait	5	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	2288	752	00 00 06 74 00 00 00 00 00 fd 09 00 fd fd 09 00 51 fd 0f fd fd 0c 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 30 fd 02 00 00 00 00 00 30 fd 02 00 00 00 00 fd 62 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 0f 75 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 83 1b 00 00 00 00 00 76 7b 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 0b fd 04 00 00 00 00	tQBB?$@AZb00buv{@	success or wait	1	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.tmp.dmp	14440	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER172A.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 64 00 00 00 68 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 <dhT8T=\H	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.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	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 32 00 33 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>2368</Pid>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1002	158	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 57 00 69 00 6e 00 33 00 32 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 50 00 53 00 45 00 2e 00 31 00 47 00 38 00 30 00 47 00 36 00 58 00 2e 00 37 00 32 00 31 00 36 00 2e 00 31 00 35 00 30 00 37 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe</ImageName>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1160	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1164	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1168	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1258	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1262	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1266	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 35 00 34 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1541</Uptime>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1316	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	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1398	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1402	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1406	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1458	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1462	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1466	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1510	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1514	2	09 00		success or wait	3	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1520	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 38 00 30 00 37 00 31 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>18071552</PeakVirtualSize>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1606	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1610	2	09 00		success or wait	3	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1616	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 34 00 31 00 31 00 30 00 37 00 32 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>14110720</VirtualSize>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1696	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 30 00 38 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>1085</PageFaultCount>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1770	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1774	2	09 00		success or wait	3	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1780	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 34 00 30 00 39 00 31 00 39 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>4091904</PeakWorkingSetSize>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1876	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1880	2	09 00		success or wait	3	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1886	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 34 00 30 00 39 00 31 00 39 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>4091904</WorkingSetSize>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1966	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1970	2	09 00		success or wait	3	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	1976	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 34 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>34456</QuotaPeakPagedPoolUsage>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2088	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2092	2	09 00		success or wait	3	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2098	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 36 00 35 00 34 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>26544</QuotaPagedPoolUsage>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2194	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2198	2	09 00		success or wait	3	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2204	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 37 00 38 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>7856</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2326	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2330	2	09 00		success or wait	3	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2336	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 35 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>7584</QuotaNonPagedPoolUsage>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2442	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2446	2	09 00		success or wait	3	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2452	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 33 00 32 00 34 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>532480</PagefileUsage>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2526	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2530	2	09 00		success or wait	3	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2536	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 34 00 30 00 36 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>540672</PeakPagefileUsage>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2626	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2630	2	09 00		success or wait	3	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2636	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 33 00 32 00 34 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>532480</PrivateUsage>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2706	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2710	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2714	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2760	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2764	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2768	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2798	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2802	2	09 00		success or wait	3	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2808	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2848	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2852	2	09 00		success or wait	4	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2860	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2890	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2894	2	09 00		success or wait	4	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2902	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2972	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2976	2	09 00		success or wait	4	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	2984	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3086	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 31 00 39 00 39 00 35 00 35 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4199557</Uptime>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3134	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3138	2	09 00		success or wait	4	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3146	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3224	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3228	2	09 00		success or wait	4	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3236	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3288	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3292	2	09 00		success or wait	4	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3300	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3344	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3348	2	09 00		success or wait	5	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3358	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3448	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3452	2	09 00		success or wait	5	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3462	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3536	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3540	2	09 00		success or wait	5	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3550	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 38 00 35 00 30 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>58509</PageFaultCount>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3626	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3630	2	09 00		success or wait	5	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3640	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 32 00 39 00 30 00 37 00 35 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>121290752</PeakWorkingSetSize>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3740	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3744	2	09 00		success or wait	5	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3754	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 31 00 37 00 30 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>121217024</WorkingSetSize>	success or wait	1	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3838	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3842	2	09 00		success or wait	5	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3852	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 34 00 32 00 39 00 35 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>11429 52</QuotaPeakPagedPoolUsage>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3968	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3972	2	09 00		success or wait	5	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	3982	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 37 00 39 00 38 00 37 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 >1079872</ QuotaPagedPoolUsage>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4082	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4086	2	09 00		success or wait	5	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4096	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 32 00 35 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>92 528</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4220	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4224	2	09 00		success or wait	5	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4234	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 39 00 39 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>79968< /QuotaNonPagedPoolUsage>	success or wait	1	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4342	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4346	2	09 00		success or wait	5	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4356	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 34 00 37 00 38 00 34 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4447846</PagefileUsage>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4434	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4438	2	09 00		success or wait	5	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4448	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 36 00 39 00 34 00 34 00 30 00 30 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>46694400</PeakPagefileUsage>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4542	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4546	2	09 00		success or wait	5	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4556	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 34 00 37 00 38 00 34 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>44478464</PrivateUsage>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4630	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4634	2	09 00		success or wait	4	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4642	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4688	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4692	2	09 00		success or wait	3	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4698	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4740	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4744	2	09 00		success or wait	2	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4748	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4780	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4784	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4786	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4828	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4832	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4834	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4872	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4876	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4880	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4942	4	0d 00 0a 00		success or wait	8	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4946	2	09 00		success or wait	16	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	4950	162	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 53 00 65 00 63 00 75 00 72 00 69 00 74 00 65 00 49 00 6e 00 66 00 6f 00 2e 00 63 00 6f 00 6d 00 2e 00 57 00 69 00 6e 00 33 00 32 00 2e 00 54 00 72 00 6f 00 6a 00 61 00 6e 00 2e 00 50 00 53 00 45 00 2e 00 31 00 47 00 38 00 30 00 47 00 36 00 58 00 2e 00 37 00 32 00 31 00 36 00 2e 00 31 00 35 00 30 00 37 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>SecuriteInfo.com.Win32.Trojan.PSE.1G80G6X.7216.15072.exe</Parameter0>	success or wait	8	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	5678	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	5682	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	5684	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	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	5724	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	5728	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	5730	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	5768	4	0d 00 0a 00		success or wait	6	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	5772	2	09 00		success or wait	12	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	5776	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6330	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6334	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6336	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6376	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6380	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6382	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6420	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6424	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6428	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6522	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6526	2	09 00		success or wait	2	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6530	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 76 00 61 00 77 00 62 00 75 00 71 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>vawbuq, Inc.</SystemManufacturer>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6644	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 76 00 61 00 77 00 62 00 75 00 71 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>vawbuq7,1</SystemProductName>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6740	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6744	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6748	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6868	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6872	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6876	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 39 00 37 00 39 00 39 00 37 00 36 00 30 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>1619799760</OSInstallDate>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6958	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6962	2	09 00		success or wait	2	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	6966	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7068	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7072	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7076	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7144	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7148	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7150	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7190	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7194	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7196	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7230	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7234	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7238	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7334	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7338	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7340	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	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7376	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7380	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7382	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7406	4	0d 00 0a 00		success or wait	3	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7410	2	09 00		success or wait	6	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7414	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7658	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7662	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7664	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7690	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7694	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7696	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 34 00 37 00 3a 00 35 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-02-08T03:47:54Z">	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7796	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7800	2	09 00		success or wait	2	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	7804	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 32 00 38 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 33 00 36 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 38 00 37 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 38 00 37 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="281" PID="2368" UptimeMS="187" TimeSinceCreationMS="187" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8062	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8066	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8070	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8090	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8094	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8096	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8134	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8138	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8140	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8178	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8182	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8186	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 62 00 38 00 65 00 62 00 35 00 34 00 34 00 2d 00 37 00 61 00 30 00 37 00 2d 00 34 00 32 00 39 00 30 00 2d 00 62 00 66 00 65 00 32 00 2d 00 37 00 32 00 65 00 34 00 62 00 36 00 33 00 32 00 35 00 64 00 38 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>2b8eb544-7a07-4290-bfe2-72e4b6325d86</Guid>	success or wait	1	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8284	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8288	2	09 00		success or wait	2	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8292	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 34 00 37 00 3a 00 35 00 34 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>2023-02-08T03:47:54Z</CreationTime>	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8390	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8394	2	09 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8396	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8436	4	0d 00 0a 00		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17F6.tmp.WERInternalMetadata.xml	8440	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	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1864.tmp.xml	0	4813	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_8b8aab2d3044b37bde8ae2665b0819910cdd8be_7335685e_095836a8\Report.wer	0	2	fd fd		success or wait	1	6C9D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_8b8aab2d3044b37bde8ae2665b0819910cdd8be_7335685e_095836a8\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	6C9D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SecuriteInfo.com_8b8aab2d3044b37bde8ae2665b0819910cdd8be_7335685e_095836a8\Report.wer	8046	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 32 00 30 00 37 00 34 00 34 00 33 00 33 00 34 00 31 00 34 00	MetadataHash=2074433414	success or wait	1	6C9D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	success or wait	1	6C9F36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6C9F1FB2	RegCreateKeyExW
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C9D43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	ProgramId	unicode	000694782bfd1fa14214741a3dac587c3ec90000ffff	success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	FileId	unicode	00006ebe1f86e07fb3fbc79e518bc6d8eb02913b11e1	success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	LowerCaseLongPath	unicode	c:\users\user\desktop\securiteinfo.com.win32.trojan.pse.1g80g6x.7216.15072.exe	success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	LongPathHash	unicode	securiteinfo.com|74c31352	success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	Name	unicode	securiteinfo.com.win32.trojan.pse.1g80g6x.7216.15072.exe	success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	Publisher	unicode		success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	Version	unicode		success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	BinFileVersion	unicode		success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	BinaryType	unicode	pe32_i386	success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	ProductName	unicode		success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	ProductVersion	unicode		success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	LinkDate	unicode	01/27/2011 10:43:15	success or wait	1	6C9F36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	BinProductVersion	unicode		success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	Size	B	00 A4 12 00 00 00 00 00	success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	Language	dword	0	success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	IsPeFile	dword	1	success or wait	1	6C9F36BF	unknown
\REGISTRY\A\{d0002fcf-02a9-b331-d719-93ce42d98bee}\Root\InventoryApplicationFile\securiteinfo.com|74c31352	IsOsComponent	dword	0	success or wait	1	6C9F36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 E6 A2 5F 09 02 00 00 00 00 00 00 00 E6 A2 5F 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6C9F1FE8	RegSetValueExW

Disassembly

No disassembly