ID: 552971
Sample Name:
SecuriteInfo.com.Variant.Bulz.785643.17886.29229
Cookbook: default.jbs
Time: 00:16:43
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

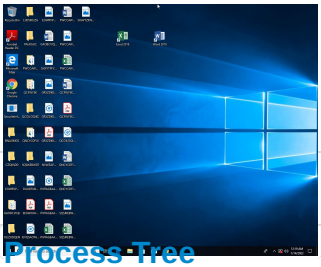
Windows Analysis Report SecuriteInfo.com.Variant.Bulz…

Overview

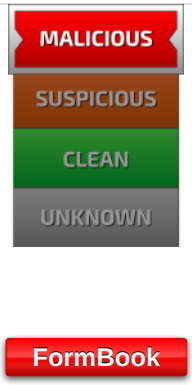
General Information

Sample Name:	SecuriteInfo.com.Variant.Bulz.785643.17886.29229 (renamed file extension from 29229 to exe)
Analysis ID:	552971
MD5:	83ac585e99b527..
SHA1:	a576a927b067c9..
SHA256:	9e2502b3945f314.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

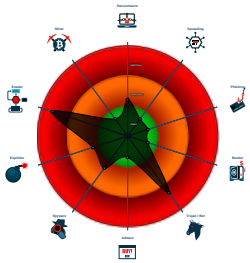


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Tries to detect virtualization through…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Variant.Bulz.785643.17886.exe (PID: 7128 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.785643.17886.exe" MD5: 83AC585E99B527EEB278702F8F711568)
  - SecuriteInfo.com.Variant.Bulz.785643.17886.exe (PID: 5636 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.785643.17886.exe MD5: 83AC585E99B527EEB278702F8F711568)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.topeasyip.company/i5nb/"
  ],
  "decoy": [
    "integratedheartspsychology.com",
    "tappsis.land",
    "norfg.com",
    "1531700.win",
    "oneplusoneexperience.com",
    "circlessalaries.com",
    "tlcremodelingcompany.com",
    "susalud.info",
    "liyanghua.club",
    "pink-zemi.com",
    "orphe.biz",
    "themodelclarified.com",
    "candidate.tools",
    "morotrip.com",
    "d2dfms.com",
    "leisuresabah.com",
    "bjbwx114.com",
    "lz-fcaini1718-hw0917-bs.xyz",
    "at-commerce-co.net",
    "buymypolicy.net",
    "5151vip73.com",
    "rentglide.com",
    "louiecruzbeltran.info",
    "lanabasargina.com",
    "lakeforestparkapartments.com",
    "guangkaiyinwu.com",
    "bornthin.com",
    "restaurantkitchenbuilders.com",
    "ecommerceoptimise.com",
    "datahk99.com",
    "markfwalker.com",
    "granitowawarszawa.com",
    "theyouthwave.com",
    "iabg.xyz",
    "jholbrook.com",
    "bsc.promo",
    "xn--grlitzerseebhne-8sb7i.com",
    "cafeteriasula.com",
    "plushcrispies.com",
    "dedicatedvirtualassistance.com",
    "ventura-taxi.com",
    "thoethertb434-ocn.xyz",
    "ylhwcl.com",
    "bigsyncmusic.biz",
    "terapiaholisticaemformacao.com",
    "comidies.com",
    "171diproad.com",
    "07dgj.xyz",
    "vppaintllc.com",
    "thepatriottutor.com",
    "wxfive.com",
    "ceinpsico.com",
    "tuningelement.store",
    "asinment.com",
    "diafraz.xyz",
    "8crhnwh658ga.biz",
    "redwolf-tech.com",
    "ksherfan.com",
    "sensationalshroom.com",
    "buy-instagram-followers.net",
    "treeserviceconsulting.com",
    "vnln.space",
    "kate-films.com",
    "selfmeta.club"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000000.299984624.000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000C.00000000.299984624.000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac6a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000C.00000000.299984624.000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.302962488.00000000033D3000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.302905715.0000000003391000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.33c02a4.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
12.2.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
12.2.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac6a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
12.2.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
12.0.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.400000.6.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 24 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

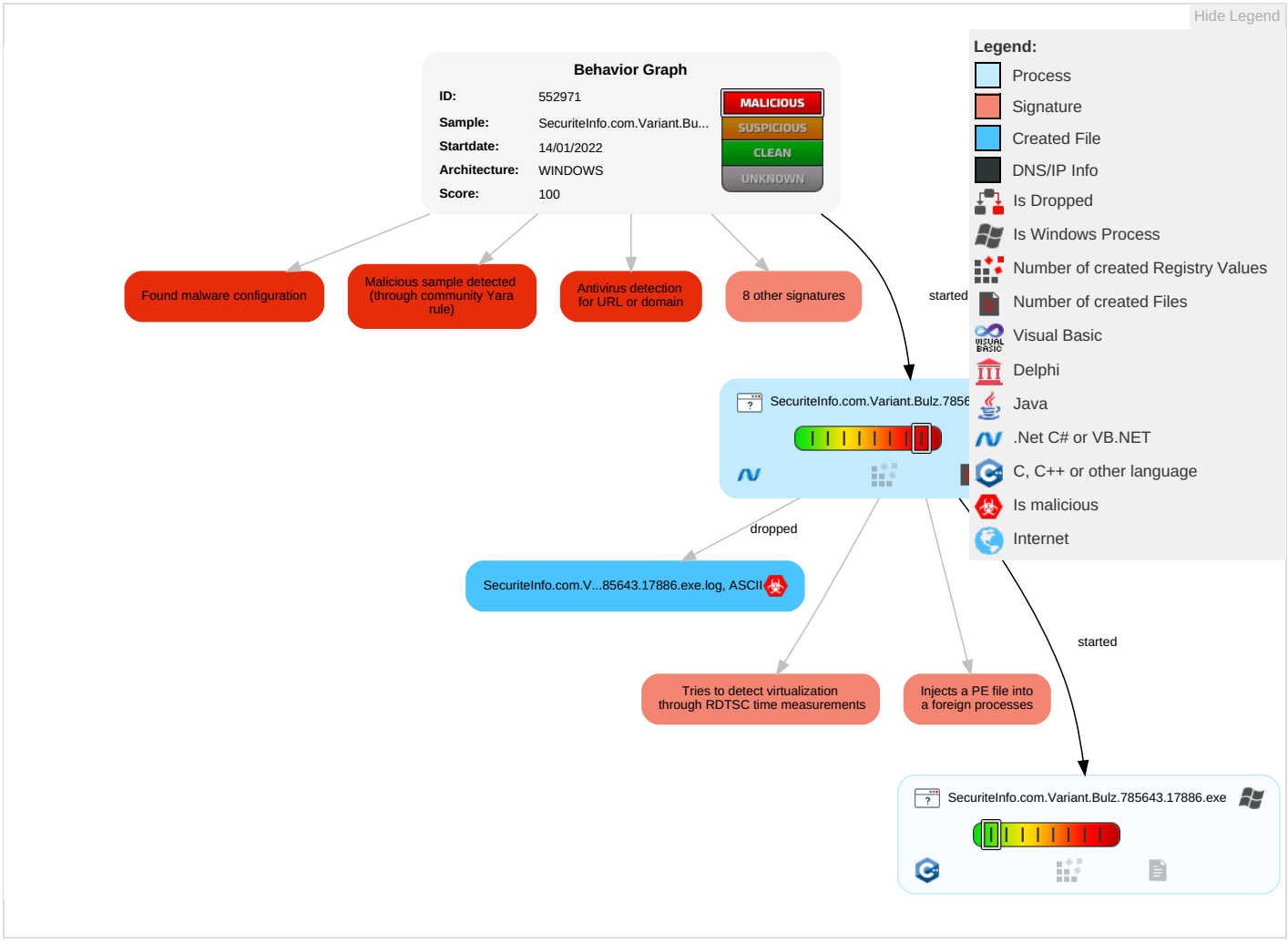
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 1	Masquerading 1	Input Capture 1	Security Software Discovery 2 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Dev Location

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	System Information Discovery 1 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access Po

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.Variant.Bulz.785643.17886.exe	43%	Virustotal		Browse
SecuriteInfo.com.Variant.Bulz.785643.17886.exe	44%	ReversingLabs	ByteCode-MSIL.Trojan.Bulz	
SecuriteInfo.com.Variant.Bulz.785643.17886.exe	100%	Avira	HEUR/AGEN.1211287	
SecuriteInfo.com.Variant.Bulz.785643.17886.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.0.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.f90000.3.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
12.2.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.f90000.1.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
12.0.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
12.0.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.f90000.2.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
0.0.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.d60000.0.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
12.0.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.f90000.0.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
0.2.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.d60000.0.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
12.0.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.f90000.7.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
12.0.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.f90000.9.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
12.0.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.f90000.1.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
12.0.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.2.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.0.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.f90000.5.unpack	100%	Avira	HEUR/AGEN.1211287		Download File
12.0.SecuriteInfo.com.Variant.Bulz.785643.17886.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
www.topeasyip.company/i5nb/	4%	Virustotal		Browse
www.topeasyip.company/i5nb/	100%	Avira URL Cloud	malware	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.topeasyip.company/i5nb/	true	• 4%, Virustotal, Browse • Avira URL Cloud: malware	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552971
Start date:	14.01.2022
Start time:	00:16:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Bulz.785643.17886.29229 (renamed file extension from 29229 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@3/1@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 8.1% (good quality ratio 5.8%) • Quality average: 52% • Quality standard deviation: 39.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
00:17:43	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Variant.Bulz.785643.17886.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Variant.Bulz.785643.17886.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.785643.17886.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzQ
MD5:	A9EFF9253CAF99EC8665E41D736DDAED
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.729098788142576
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SecuriteInfo.com.Variant.Bulz.785643.17886.exe
File size:	417792
MD5:	83ac585e99b527eeb278702f8f711568
SHA1:	a576a927b067c94cdbc1e7b353f60577f5b310f9
SHA256:	9e2502b3945f31482623e8e61dcb85b9ebb7d9a4244d9074fa289596c9da513e
SHA512:	f4a5f197cca552237ca4ca0dbdba4af5e5c0f6bca7a05313a61d96c5021049edeb0b38d8e4ad5ee3b062692038f05254787a57c5c1a0e951e9a9b9f091a304ac
SSDEEP:	12288:gyK777777777777OPMfcmnxTLrXEQ0/Ll1PishiMkNMfPjJ8W:jK777777777777OKLQR1Pf+aP6W
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H?.a.....V.....:u... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46753a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61E03F48 [Thu Jan 13 15:03:36 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x65540	0x65600	False	0.877254161529	data	7.74258433139	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x68000	0x598	0x600	False	0.426432291667	data	4.37535552335	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Variant.Bulz.785643.17886.exe PID: 7128 Parent PID: 3428

General

Start time:	00:17:34
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.785643.17886.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.785643.17886.exe"
Imagebase:	0xd60000
File size:	417792 bytes
MD5 hash:	83AC585E99B527EEB278702F8F711568
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.302962488.00000000033D3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.302905715.0000000003391000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.303196855.0000000004399000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.303196855.0000000004399000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.303196855.0000000004399000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: SecuriteInfo.com.Variant.Bulz.785643.17886.exe PID: 5636 Parent PID: 7128

General

Start time:	00:17:43
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.785643.17886.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.785643.17886.exe
Imagebase:	0xf90000
File size:	417792 bytes
MD5 hash:	83AC585E99B527EEB278702F8F711568
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000000.299984624.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000000.299984624.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000000.299984624.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.302341566.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.302341566.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.302341566.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000000.300583047.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000000.300583047.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000000.300583047.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Disassembly

Code Analysis