ID: 433042
Sample Name:
SecuriteInfo.com.Variant.Bulz.349164.25568.5993
Cookbook: default.jbs
Time: 08:06:38
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

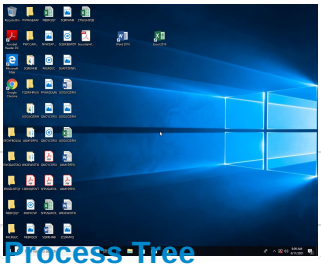
Analysis Report SecuriteInfo.com.Variant.Bulz.349164.2…

Overview

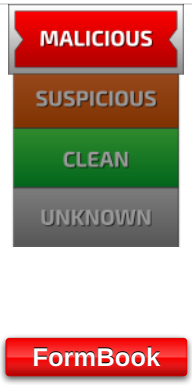
General Information

Sample Name:	SecuriteInfo.com.Variant.Bulz.349164.25568.5993 (renamed file extension from 5993 to exe)
Analysis ID:	433042
MD5:	c66fe399ec0cb59..
SHA1:	fcc9984283b3596..
SHA256:	57f599e4ae63304.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

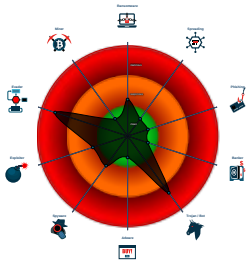


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected FormBook
- .NET source code contains method …
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Antivirus or Machine Learning detec…
- Checks if the current process is bein…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Variant.Bulz.349164.25568.exe (PID: 6776 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.349164.25568.exe' MD5: C66FE399EC0CB598B2167A348C17F6A2)
  - SecuriteInfo.com.Variant.Bulz.349164.25568.exe (PID: 6968 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.349164.25568.exe MD5: C66FE399EC0CB598B2167A348C17F6A2)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.rep.place/pba2/"
  ],
  "decoy": [
    "marshabenjamin.com",
    "ipx-tv.com",
    "1826bet.net",
    "free-story-civilizatiom.com",
    "projecteightstudio.com",
    "blaxies3.com",
    "knowyourpharmacy.com",
    "daviddelavariservices.space",
    "hawaiidreamevents.com",
    "chickdeal.net",
    "toko363.com",
    "flextech.design",
    "americanprimativeguitar.com",
    "sourcesfloor.com",
    "project6212.com",
    "eggbeaterhub.xyz",
    "homefittness.com",
    "eigenguard.com",
    "bridgessd.com",
    "wordabbler.com",
    "432524.com",
    "blumlifestyle.com",
    "cn-liangyu.com",
    "earwaxsux.com",
    "n2keg.com",
    "kthetwobrothers.com",
    "freetoplaymedia.com",
    "ncunlimited.com",
    "mckinleygroupcommandforyou.com",
    "y-beautyplus.com",
    "plny.xyz",
    "luckyliars.com",
    "succozero.com",
    "zoorack.net",
    "myloveclubs.com",
    "cashstreamsonline.club",
    "23237a2371.info",
    "live-now20.xyz",
    "followtea.com",
    "xn--vhqqb70qmrhwmvnh0e.xyz",
    "thocudian.net",
    "trueradiencesolutions.net",
    "dictionarykick.com",
    "banbochfm.com",
    "privacyphonecover.com",
    "towandastorage.com",
    "livingthesustainablelife.com",
    "freeagencevoyage.com",
    "veritasfertilityandsurgery.com",
    "thehindufestival.com",
    "ollipsisparents.com",
    "caphesachnguyenchat.com",
    "xn--egegncel-95a.com",
    "americanpoolnbilliards.com",
    "wonderfulwanfield.com",
    "sheya360.com",
    "solterasalos40.com",
    "astarswimschools.net",
    "vcnse.com",
    "jinshifj.com",
    "washingtonreversemtgloans.com",
    "mutieudao.online",
    "fluatrec.com",
    "maggionsurvey.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.662601270.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000000.662601270.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000000.662601270.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.664811462.0000000003EE9000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.664811462.0000000003EE9000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xc41f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xc4582:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x2b0178:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x2b0502:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xd0295:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x2bc215:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xcfd81:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x2bbd01:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xd0397:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x2bc317:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xd050f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x2bc48f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xc4f9a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x2b0f1a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xceffc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x2baf7c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xc5d12:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x2b1c92:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xd5387:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x2c1307:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xd642a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.SecuriteInfo.com.Variant.Bulz.349164.25568.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.SecuriteInfo.com.Variant.Bulz.349164.25568.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.0.SecuriteInfo.com.Variant.Bulz.349164.25568.exe.400000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
3.2.SecuriteInfo.com.Variant.Bulz.349164.25568.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
3.2.SecuriteInfo.com.Variant.Bulz.349164.25568.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

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 method to dynamically call methods (often used by packers)

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

Stealing of Sensitive Information:

Yara detected FormBook

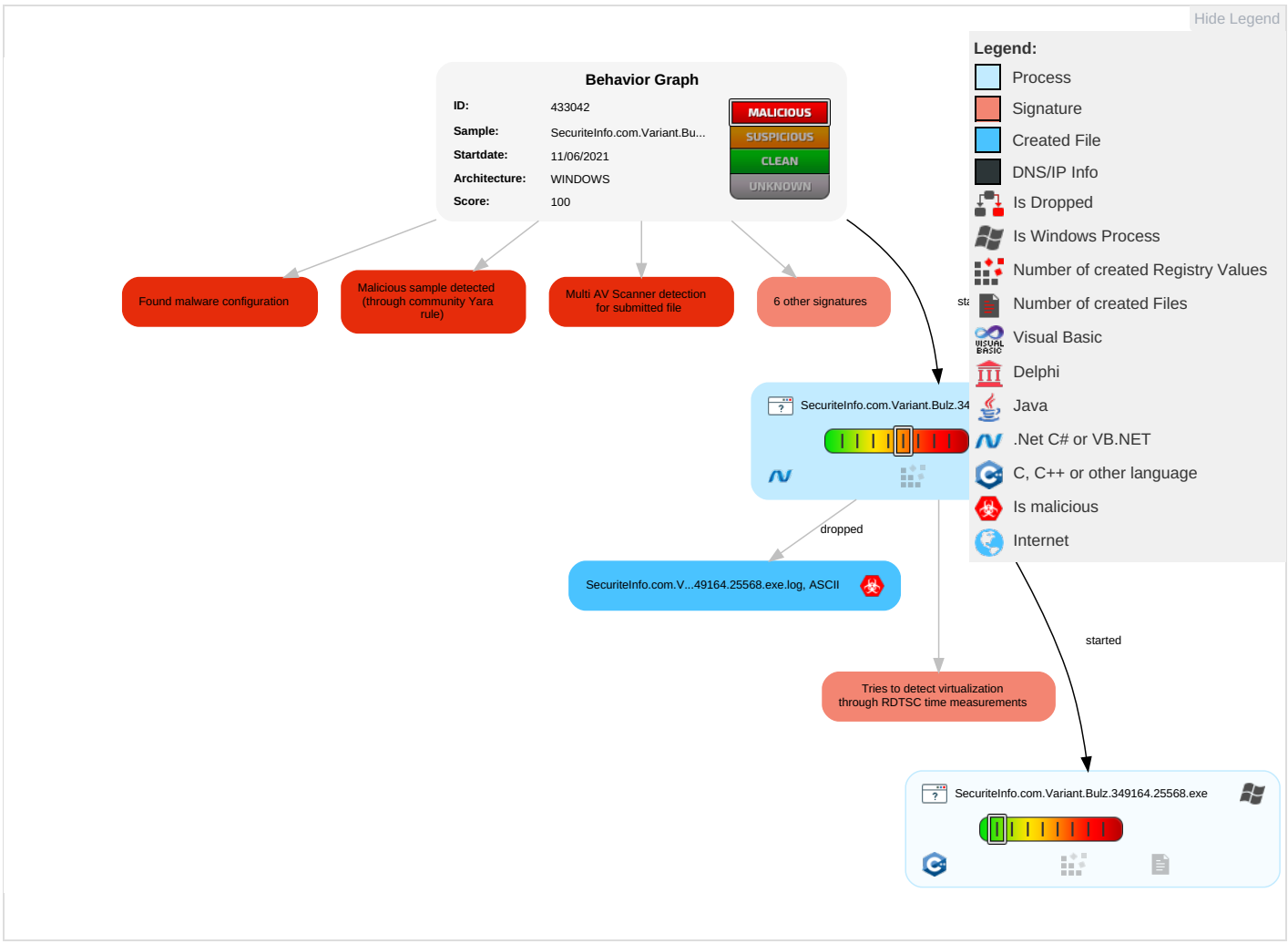
Remote Access Functionality:

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	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
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	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 t Redirect Pho 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 SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 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 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
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 or 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-Fi Access Point

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.349164.25568.exe	46%	Virustotal		Browse
SecuriteInfo.com.Variant.Bulz.349164.25568.exe	35%	ReversingLabs	Win32.Trojan.Wacatac	
SecuriteInfo.com.Variant.Bulz.349164.25568.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.SecuriteInfo.com.Variant.Bulz.349164.25568.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.SecuriteInfo.com.Variant.Bulz.349164.25568.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.rep.place/pba2/	2%	Virustotal		Browse
www.rep.place/pba2/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.rep.place/pba2/	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433042
Start date:	11.06.2021
Start time:	08:06:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Bulz.349164.25568.5993 (renamed file extension from 5993 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:	21
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:	Failed
HDC Information:	• Successful, ratio: 6.6% (good quality ratio 6.1%) • Quality average: 74.4% • Quality standard deviation: 30.5%
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
08:07:32	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Variant.Bulz.349164.25568.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.349164.25568.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.349164.25568.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.40623038199471
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	SecuriteInfo.com.Variant.Bulz.349164.25568.exe
File size:	1011200
MD5:	c66fe399ec0cb598b2167a348c17f6a2
SHA1:	fcc9984283b3596fb575523fb90eb80ce702abe2
SHA256:	57f599e4ae63304de5795909f694122665f7c492df8078f7c5abb084d09baa2d
SHA512:	59993980767c12bb6e536a0ba4ab60b5ea54987a3893fd4044b1078d4f7014304e6e2c147488a138f57342eaba1bca5ec8842753b5bd3ab48360d8b9458598d8
SSDEEP:	24576:6tN220KdM+IT+hwWVAQSW3+0NeBUdtX1q:yDRl0V9N3JwBUE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...z..`.....V.....2... ...@....@.. .....@.....

File Icon

Icon Hash:	c4c4c4c8ccd4d0c4

Static PE Info

General

Entrypoint:	0x4c328e
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:	0x60C2AA7A [Fri Jun 11 00:12:42 2021 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	0xc1294	0xc1400	False	0.897193109234	data	7.85673320535	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.sdata	0xc4000	0x1e8	0x200	False	0.861328125	data	6.62325644136	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc6000	0x35134	0x35200	False	0.210225183824	data	4.44239053634	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfc000	0xc	0x200	False	0.044921875	data	0.0980041756627	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.349164.25568.exe PID: 6776 Parent PID: 6108

General

Start time:	08:07:30
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.349164.25568.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.349164.25568.exe'
Imagebase:	0xac0000
File size:	1011200 bytes
MD5 hash:	C66FE399EC0CB598B2167A348C17F6A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.664811462.0000000003EE9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.664811462.0000000003EE9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.664811462.0000000003EE9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.664247776.0000000002F1F000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: SecuriteInfo.com.Variant.Bulz.349164.25568.exe PID: 6968 Parent PID: 6776

General

Start time:	08:07:34
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.349164.25568.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.349164.25568.exe
Imagebase:	0xeb0000
File size:	1011200 bytes
MD5 hash:	C66FE399EC0CB598B2167A348C17F6A2
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: 00000003.00000000.662601270.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.662601270.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.662601270.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.664522711.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.664522711.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.664522711.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Disassembly

Code Analysis