ID: 255764
Sample Name:
SecuriteInfo.com.Trojan.GenericKD.34263609.3735.31368
Cookbook: default.jbs
Time: 01:31:09
Date: 02/08/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

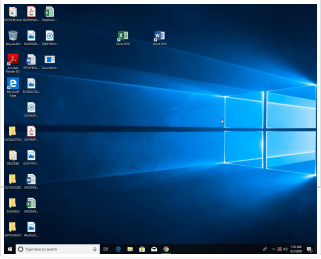
Analysis Report SecuriteInfo.com.Trojan.GenericKD.342…

Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.GenericKD.34263609.3735.31368 (renamed file extension from 31368 to exe)
Analysis ID:	255764
MD5:	2112c999e44a7d..
SHA1:	9969d4de902cbe..
SHA256:	c4d62fb1cf19280..

Most interesting Screenshot:



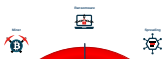
Detection

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Yara detected AntiVM_3
- Yara detected FormBook
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Checks if the current process is bein…
- Contains functionality for execution …
- Contains functionality to access load…
- Contains functionality to call native f…
- Contains functionality to read the PEB

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe (PID: 7112 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe' MD5: 2112C999E44A7D4180680068D9FFB6B1)
  - SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe (PID: 7148 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe MD5: 2112C999E44A7D4180680068D9FFB6B1)
  - SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe (PID: 7160 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe MD5: 2112C999E44A7D4180680068D9FFB6B1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.238874448.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.238874448.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98b8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b22:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x157a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15291:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x158a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x15a1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa69a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1450c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb393:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
00000002.00000002.238874448.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18429:$sqlite3step: 68 34 1C 7B E1 • 0x1853c:$sqlite3step: 68 34 1C 7B E1 • 0x18458:$sqlite3text: 68 38 2A 90 C5 • 0x1857d:$sqlite3text: 68 38 2A 90 C5 • 0x1846b:$sqlite3blob: 68 53 D8 7F 8C • 0x18593:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.238632327.0000000003336000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.238799313.00000000042F1000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 7 entries				

Unpacked PEs

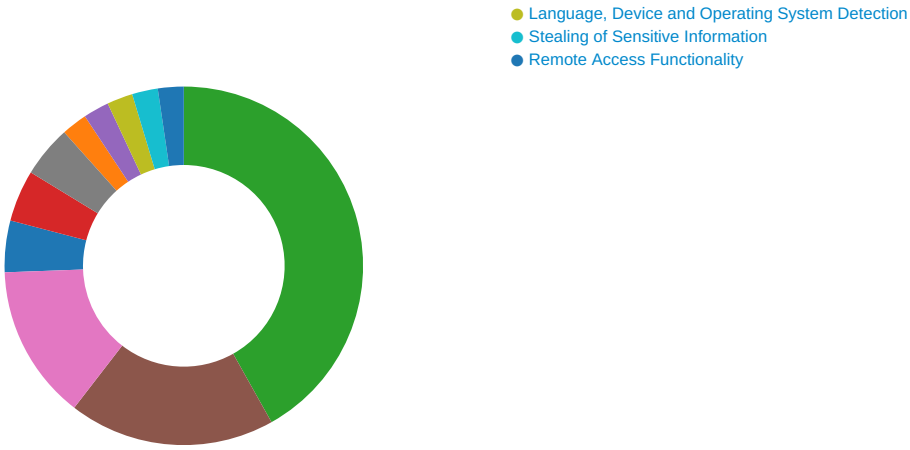
Source	Rule	Description	Author	Strings
2.2.SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ab8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d22:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x149a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14491:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14aa7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14c1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x989a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1370c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa593:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19d17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ad1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17629:$sqlite3step: 68 34 1C 7B E1 • 0x1773c:$sqlite3step: 68 34 1C 7B E1 • 0x17658:$sqlite3text: 68 38 2A 90 C5 • 0x1777d:$sqlite3text: 68 38 2A 90 C5 • 0x1766b:$sqlite3blob: 68 53 D8 7F 8C • 0x17793:$sqlite3blob: 68 53 D8 7F 8C
2.2.SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98b8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b22:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x157a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15291:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x158a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x15a1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa69a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1450c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb393:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion



Click to jump to signature section

AV Detection:

Yara detected FormBook

Machine Learning detection for sample

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

Yara detected AntiVM_3

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:

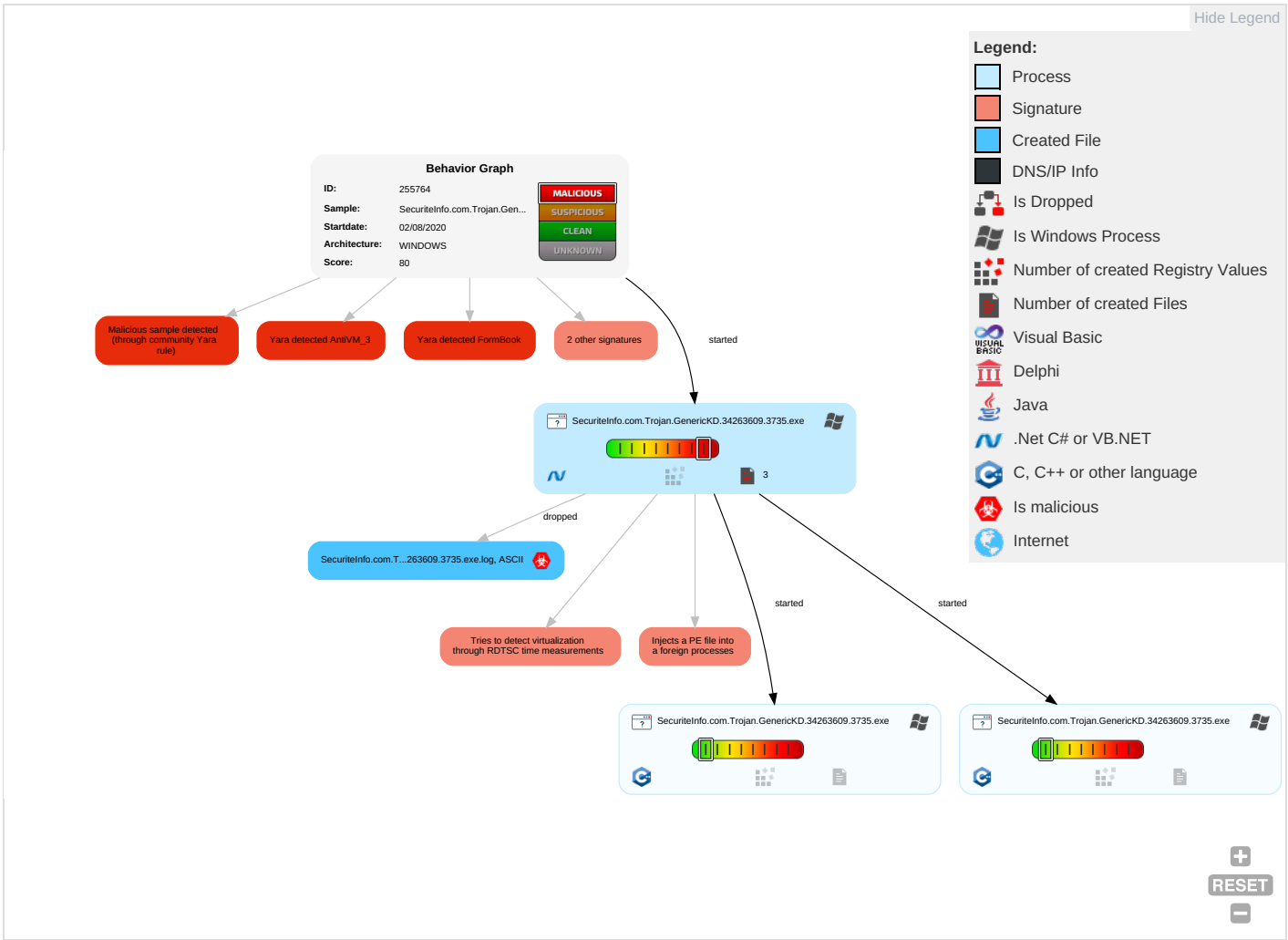
Yara detected FormBook

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	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2	NTDS	System Information Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	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	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access P

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	255764
Start date:	02.08.2020
Start time:	01:31:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.GenericKD.34263609.3735.31368 (renamed file extension from 31368 to exe)
Cookbook file name:	default.jbs
Analysis system description:	w10x64 Windows 10 64 bit v1803 with Office Professional Plus 2016, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	3
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:	mal80.troj.evad.winEXE@5/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 7.5% (good quality ratio 6.6%) • Quality average: 67.8% • Quality standard deviation: 31.7%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

Simulations

Behavior and APIs

Time	Type	Description
01:31:58	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe modified

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.476024805108019
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • 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% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe
File size:	550912
MD5:	2112c999e44a7d4180680068d9ffb6b1
SHA1:	9969d4de902cbeae01cbc42e9ec200a919724581
SHA256:	c4d62fb1cf19280c5eefbd09de9d2f7d2c7b23abaf396cff79d552bd4363f1eb
SHA512:	6ebe999d02b847f6b805808ee19791362a7ed42c61c45c956e8cbb72b0fd287239580b12de7f99eb0c17a3ce2c535fef8578a6acd55a0256c227dfbe27b1a5d
SSDEEP:	12288:ZUgF6HFg503ApMchTthMhvbBQI2cThdJ:d6He503A75thSdQI2cThdJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....^"_.....P..\.....nz... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x487a6e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

General

Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F225EAC [Thu Jul 30 05:46:20 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x87a1c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x88000	0x638	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x85a74	0x85c00	False	0.774211448598	data	7.49063983261	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x88000	0x638	0x800	False	0.34130859375	data	3.5089487242	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x880a0	0x3ac	data		
RT_MANIFEST	0x8844c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Massapequa Public School District 2012 - 2020
Assembly Version	1.0.0.0
InternalName	wUOUZcmvlX.exe
FileVersion	1.0.0.0
CompanyName	Massapequa Public School District
LegalTrademarks	
Comments	
ProductName	Tetris
ProductVersion	1.0.0.0
FileDescription	Tetris
OriginalFilename	wUOUZcmvlX.exe

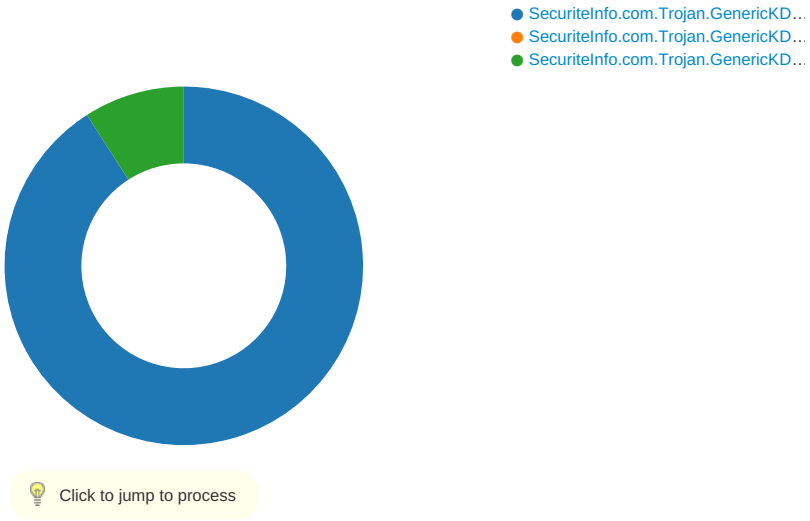
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe PID: 7112
Parent PID: 5824

General

Start time:	01:31:57
Start date:	02/08/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe'
Imagebase:	0xb80000
File size:	550912 bytes
MD5 hash:	2112C999E44A7D4180680068D9FFB6B1
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.238632327.0000000003336000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.238799313.00000000042F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.238799313.00000000042F1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.238799313.00000000042F1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.238591769.00000000032F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.238839326.0000000004346000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.238839326.0000000004346000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.238839326.0000000004346000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B260AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B260AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B134A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe.log	unknown	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	72DFA33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72B55544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72B55544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4106	success or wait	1	72B55544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72B58738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72B58738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4106	success or wait	1	72B58738	ReadFile

Analysis Process: SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe PID: 7148
Parent PID: 7112

General

Start time:	01:31:58

Start date:	02/08/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe
Imagebase:	0x10000
File size:	550912 bytes
MD5 hash:	2112C999E44A7D4180680068D9FFB6B1
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe PID: 7160
Parent PID: 7112

General

Start time:	01:31:59
Start date:	02/08/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.34263609.3735.exe
Imagebase:	0xdb0000
File size:	550912 bytes
MD5 hash:	2112C999E44A7D4180680068D9FFB6B1
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.238874448.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.238874448.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.238874448.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419927	NtReadFile

Disassembly

Code Analysis