ID: 343148
Sample Name:
SecuriteInfo.com.Generic.mg.354e60543438661b.7014
Cookbook: default.jbs
Time: 12:07:38
Date: 22/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

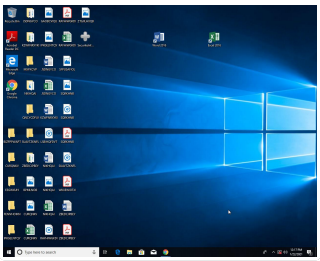
Analysis Report SecuriteInfo.com.Generic.mg.354e6054…

Overview

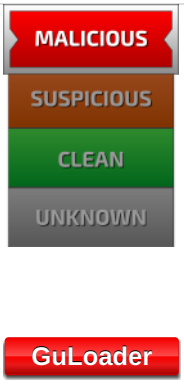
General Information

Sample Name:	SecuriteInfo.com.Generic.mg.354e60543438661b.7014 (renamed file extension from 7014 to exe)
Analysis ID:	343148
MD5:	354e6054343866..
SHA1:	f698e89c2f16c02..
SHA256:	e5aac8a58f55ef2..
Tags:	GuLoader

Most interesting Screenshot:



Detection



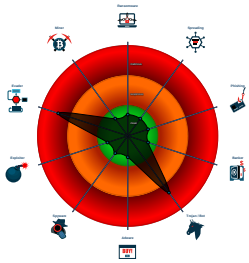
GuLoader

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to read the PEB
- PE file contains strange resources
- Sample file is different than original …
- Uses 32bit PE files
- Uses code obfuscation techniques (…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Generic.mg.354e60543438661b.exe (PID: 1340 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.354e60543438661b.exe' MD5: 354E60543438661B75246F39F6CDE70D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

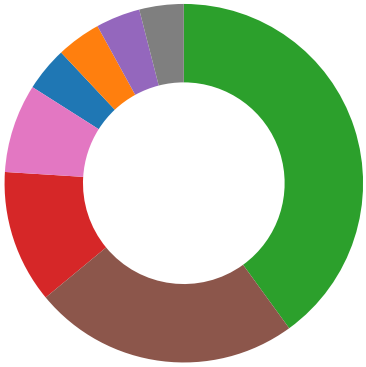
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: SecuriteInfo.com.Generic.mg.354e60543438661b.exe PID: 1340	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: SecuriteInfo.com.Generic.mg.354e60543438661b.exe PID: 1340	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

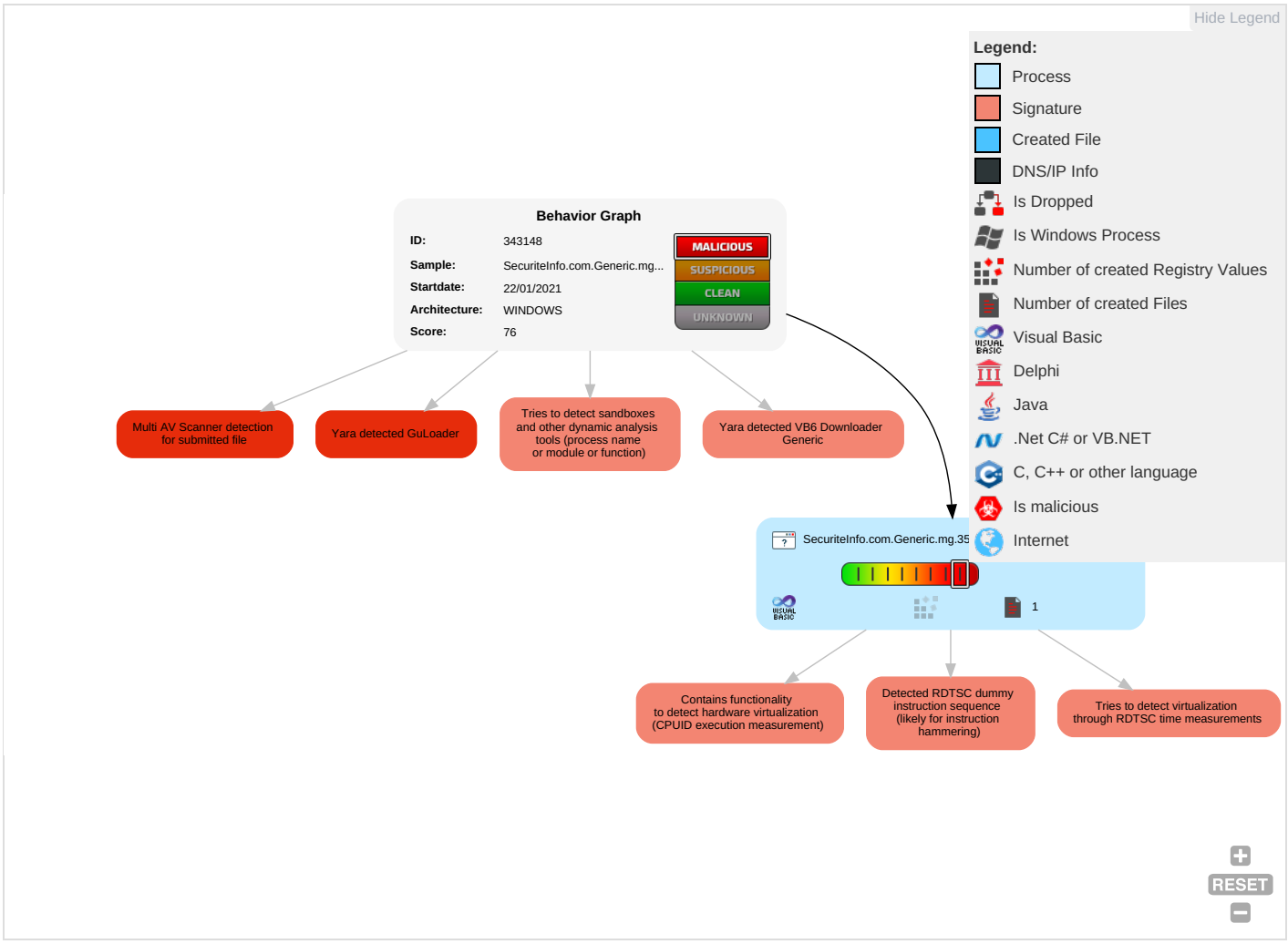
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

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
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Process Injection 1	OS Credential Dumping	Security Software Discovery 4 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

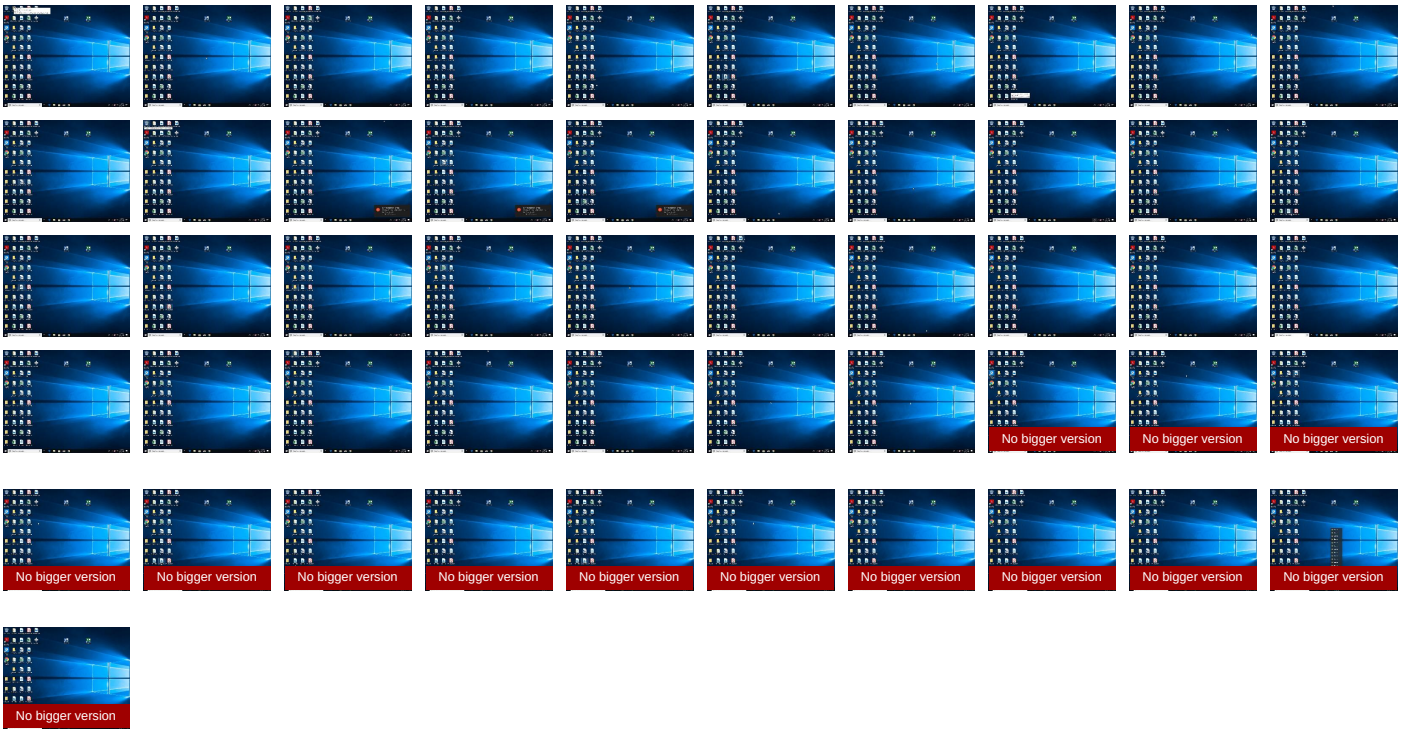
Behavior Graph



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.Generic.mg.354e60543438661b.exe	18%	Virustotal		Browse
SecuriteInfo.com.Generic.mg.354e60543438661b.exe	7%	ReversingLabs	Win32.Infostealer.Generic	

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:	31.0.0 Red Diamond
Analysis ID:	343148
Start date:	22.01.2021
Start time:	12:07:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Generic.mg.354e60543438661b.7014 (renamed file extension from 7014 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:	10
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:	mal76.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 19.1% (good quality ratio 10.5%) • Quality average: 30.8% • Quality standard deviation: 31.3%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, MusNotifyIcon.exe, conhost.exe, svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.7832273639812195
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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.Generic.mg.354e60543438661b.exe
File size:	69632
MD5:	354e60543438661b75246f39f6cde70d
SHA1:	f698e89c2f16c02de7183a2c47ac31fda700ce3c
SHA256:	e5aac8a58f55ef2a6ac7aa5997a05a240fd09d8e856f95209b7e499beb4c4d57
SHA512:	76830c145ae3d4dc481f54f8f6082a4f3342c7f3b38c484ad3130e0a91e55a3795e7a9a59f0af3591f66bb2e0a75dc5a6d2c47e5b889aef59e9460f4494d4c78
SSDEEP:	768:24XCdZhk6uHDQ6wJf1k4CtQHFRXrNMCL5g5eucYJJzx6L:tXC7QH8RJCVtQjX+CO5FcYJJzM
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....}Q.....0.....T.....@.....

File Icon

Icon Hash:	f030f0c6f030b100

Static PE Info

General

Entrypoint:	0x401354
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x517D149C [Sun Apr 28 12:22:52 2013 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	e22238527efb5691a1dfa3f0e707406a

Entrypoint Preview

Instruction
push 00401FE4h
call 00007F9F88C88BD5h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dl, bh
mov bh, byte ptr [ecx]
fdivr dword ptr [ebx-77h]
dec esi
dec ebx
wait
das
push cs
sbb eax, dword ptr [eax+0000E2DFh]
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
inc ecx
add byte ptr [esi+50018250h], al
jc 00007F9F88C88C51h
push 00000065h
arpl word ptr [ecx+esi+00h], si
add byte ptr [eax], al
add byte ptr [ecx+edi+11h], ch
add eax, dword ptr [eax]
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
add al, 02h
shr dword ptr [edi], cl
pop ecx
jle 00007F9F88C88BF1h
nop

Instruction
inc edi
test edi, ecx
xchg byte ptr [F4F67CEAh], bh
pextrw ebp, dqword ptr [ebp+0C1DBC99h], 4Dh
mov edi, 40483208h
xlatb
dec edi
pop ebx
cmp cl, byte ptr [edi-53h]
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
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
fimul word ptr [ebx]
add byte ptr [eax], al
inc edx
or eax, dword ptr [eax]
add byte ptr [eax], al
or eax, dword ptr [eax]
jo 00007F9F88C88C51h
insb
imul ebp, dword ptr [edi+72h], 65746D61h
jnc 00007F9F88C88BE2h
or eax, 46000B01h
outsd
jc 00007F9F88C88C52h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xea04	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x11000	0x938	.rsrc
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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xfc	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xde58	0xe000	False	0.534127371652	data	6.44198752835	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xf000	0x1180	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x11000	0x938	0x1000	False	0.14208984375	data	1.43341163181	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x113d0	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x113bc	0x14	data		
RT_VERSION	0x110f0	0x2cc	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaLenBstr, __vbaEnd, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaVarForInit, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaVarTstLt, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaI4Var, __vbaVarDup, __vbaFpI4, _CIatan, __vbaCastObj, __vbaStrMove, _allmul, _CItan, __vbaVarForNext, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0404 0x04b0
LegalCopyright	Calc Theory
InternalName	Altrets8
FileVersion	1.00
CompanyName	Calc Theory
Comments	Calc Theory
ProductName	Calc Theory
ProductVersion	1.00
FileDescription	Calc Theory
OriginalFilename	Altrets8.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: SecuriteInfo.com.Generic.mg.354e60543438661b.exe PID: 1340
Parent PID: 6084

General

Start time:	12:08:30
Start date:	22/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.354e60543438661b.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.354e60543438661b.exe'
Imagebase:	0x400000
File size:	69632 bytes
MD5 hash:	354E60543438661B75246F39F6CDE70D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis