ID: 345046
Sample Name:
SecuriteInfo.com.Trojan.VbCrypt.1981.29338.509
Cookbook: default.jbs
Time: 16:19:07
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report SecuriteInfo.com.Trojan.VbCrypt.1981.29338.509 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 4
Signature Overview 5
Compliance: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted IPs 8
General Information 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
File Icon 9
Static PE Info 10
General 10
Authenticode Signature 10
Entrypoint Preview 10
Data Directories 12
Sections 12
Resources 12
Imports 12
Version Infos 12
Possible Origin 13
Network Behavior 13
Code Manipulations 13
Statistics 13

System Behavior 13
Analysis Process: SecuriteInfo.com.Trojan.VbCrypt.1981.29338.exe PID: 1364 Parent PID: 5540 13
General 13
File Activities 13
Disassembly 14
Code Analysis 14

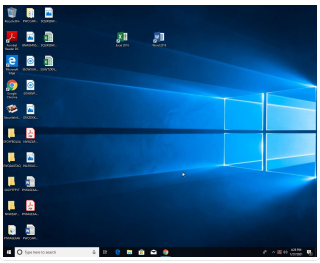
Analysis Report SecuriteInfo.com.Trojan.VbCrypt.1981.2…

Overview

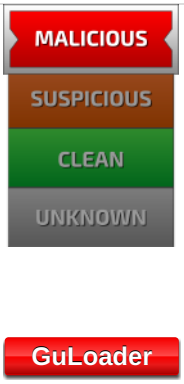
General Information

Sample Name:	SecuriteInfo.com.Trojan.VbCrypt.1981.29338.509 (renamed file extension from 509 to exe)
Analysis ID:	345046
MD5:	41e225be0600a7..
SHA1:	260d739ff434f90…
SHA256:	50851ce50dcc51…
Tags:	GuLoader

Most interesting Screenshot:



Detection



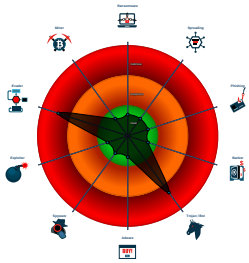
GuLoader

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected GuLoader
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- 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 call native f…
- Contains functionality to read the PEB
- PE / OLE file has an invalid certificate
- PE file contains strange resources
- Program does not show much activi…
- Sample file is different than original …

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.VbCrypt.1981.29338.exe (PID: 1364 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.VbCrypt.1981.29338.exe' MD5: 41E225BE0600A7EFD31CA3206F97EC17)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

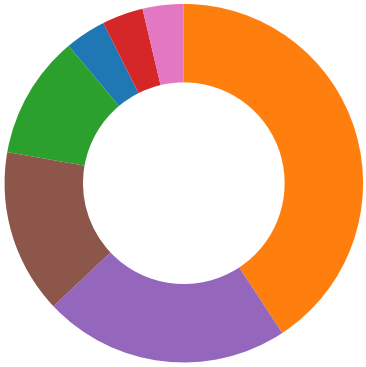
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: SecuriteInfo.com.Trojan.VbCrypt.1981.29338.exe PID: 1364	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: SecuriteInfo.com.Trojan.VbCrypt.1981.29338.exe PID: 1364	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- 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

Compliance:

Uses 32bit PE files

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

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

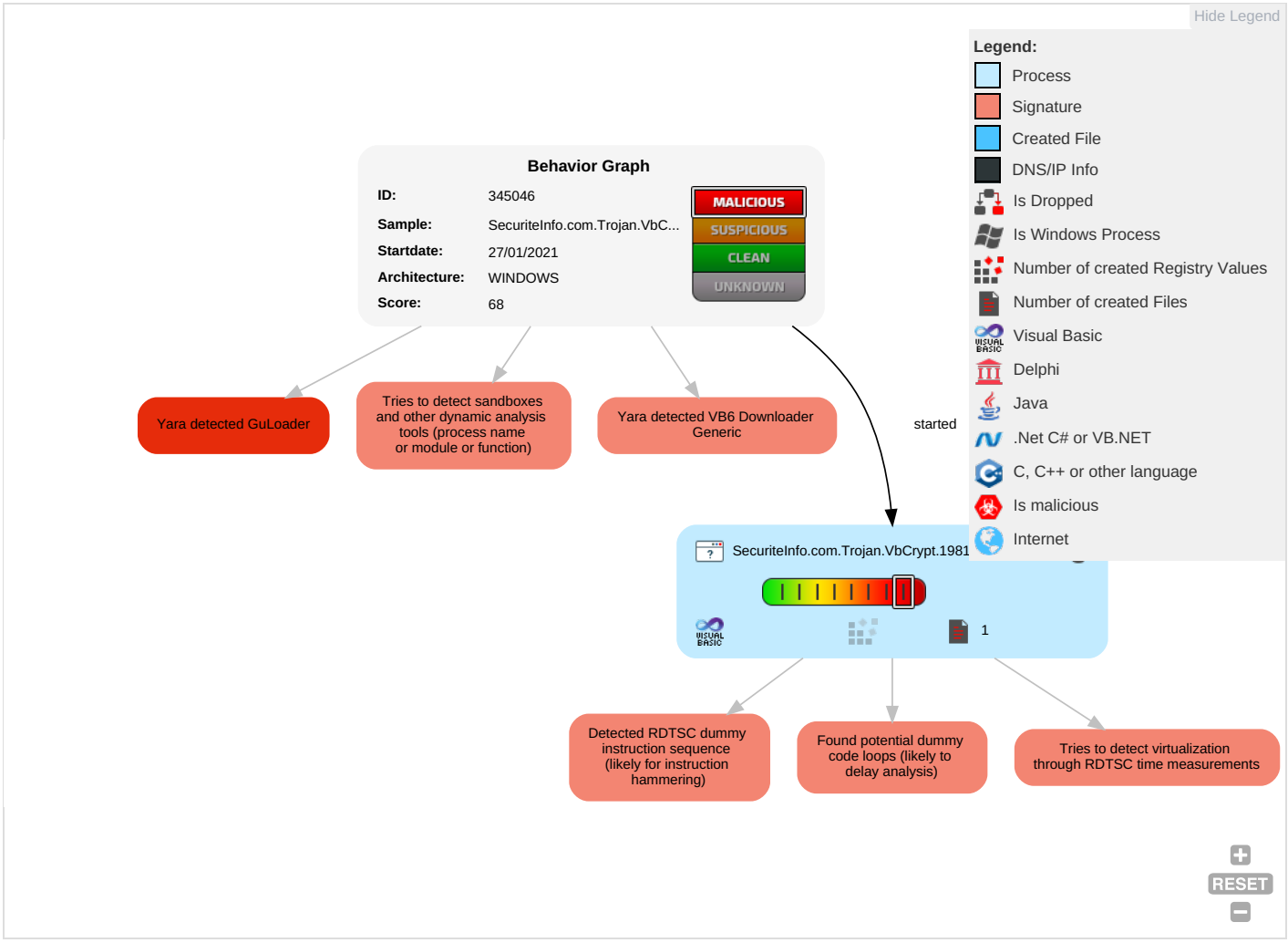
Anti Debugging:

Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 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	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

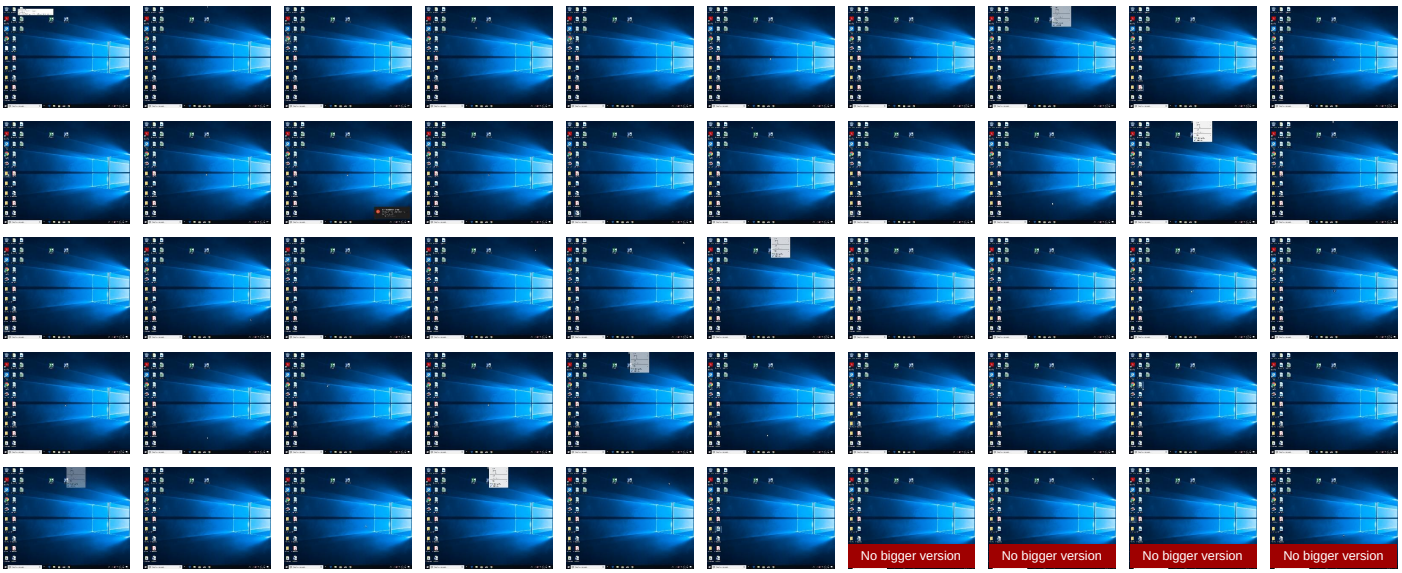
Behavior Graph



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.VbCrypt.1981.29338.exe	4%	ReversingLabs		

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 Emerald
Analysis ID:	345046
Start date:	27.01.2021
Start time:	16:19:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.VbCrypt.1981.29338.509 (renamed file extension from 509 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:	35
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:	mal68.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
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, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • VT rate limit hit for: /opt/package/joesandbox/database/analysis/345046/sample/SecuriteInfo.com.Trojan.VbCrypt.1981.29338.exe

Simulations

Behavior and APIs

No simulations
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):	5.625631069652798
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.Trojan.VbCrypt.1981.29338.exe
File size:	136968
MD5:	41e225be0600a7efd31ca3206f97ec17
SHA1:	260d739ff434f90daad6c2c724fc9333348e9007
SHA256:	50851ce50dcc51f9c8111e3071ee9b041181cd462cd263b38f28f51dbc79c38a
SHA512:	a1a20040e223f8f78ffa845a1a362ec607fbb38e4f7f34fc4f17963d7e1c5d840869a89c610c68242713b628f13c616c2fa0609bf030683566ac5735651609d4
SSDEEP:	1536:Y+bSgYX0Y7aSE2Ex8qY4l0tLOMsxDUZAKcgFlfv35O7kl8De+M:DEX0Y7aSE7xHY4l0pmDbmYkQu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a...%.u.%.u.%.u...{.$.u.j.|...u...x.$.u.Rich%.u.....PE..L....0.I.....@

File Icon

Icon Hash:	11d0cca988e43480

Static PE Info

General

Entrypoint:	0x40140c
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x491530A5 [Sat Nov 8 06:24:37 2008 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:	1e02c8ef609fc8033c11804967aa3948

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=TILLEMPER@Paulicianism7.NYS, CN=Pilandite4, OU=Hornviol, O=Rekompenserer, L=SHAHENS, S=VENTRICULITIDAE, C=CV
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 1/26/2021 2:42:15 PM 1/26/2022 2:42:15 PM
Subject Chain	• E=TILLEMPER@Paulicianism7.NYS, CN=Pilandite4, OU=Hornviol, O=Rekompenserer, L=SHAHENS, S=VENTRICULITIDAE, C=CV
Version:	3
Thumbprint MD5:	CAC4ADCD7033303DAF452FD592D6C90C
Thumbprint SHA-1:	902697F79368DD47401D961D51B32CCCB5DCA049
Thumbprint SHA-256:	A9A5C43F7DECB40E5AC1143E0D27AA012EB8812D119ADF17F00FD010F6E1E1C2
Serial:	00

Entrypoint Preview

Instruction
push 00402BFCh
call 00007FF554BA5E53h
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 byte ptr [eax-0Ch], ah
inc esp
das
sub edi, eax
lodsb
inc ecx
call far 1D55h : E02E0DA3h
pop edx
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
inc eax
adc al, ECh
add eax, dword ptr [esi+65h]
push 0000006Ch
bound esp, dword ptr [ebp+64h]
insd
je 00007FF554BA5E62h
inc ecx
add byte ptr [eax], ah
or byte ptr [ecx+00h], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
or edx, dword ptr [esi-1D27008Eh]
wait
nop
dec esi
stosd
pushfd
pop edi
pop ecx
add eax, FB7F4921h
cli
sbb dl, dh
test byte ptr [edx], bl
jmp 00007FF56149F7ADh
scasd
xchg eax, ebx
or byte ptr [edx-7Ch], al
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
pop ebp
adc byte ptr [eax], al
add byte ptr [ecx+0000000Eh], dl
push cs
add byte ptr [ebx+74h], dl

Instruction
jc 00007FF554BA5EC3h
jo 00007FF554BA5ED0h
imul ebp, dword ptr [esi+67h], 656E7265h
jnc 00007FF554BA5E62h
or eax, 6F000901h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1d324	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2a000	0x1256	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x21000	0x708	.data
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	0x238	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x140	.text
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
.text	0x1000	0x1c944	0x1d000	False	0.300604458513	data	5.94562175337	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1e000	0xb31c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2a000	0x1256	0x2000	False	0.359375	data	3.33091481892	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2a9ae	0x8a8	data		
RT_ICON	0x2a446	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x2a424	0x22	data		
RT_VERSION	0x2a120	0x304	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	__vbaStrI2, _CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaAryMove, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaRecAnsiToUni, __vbaCopyBytes, __vbaStrCat, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaLateMemSt, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaStrFixstr, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaObjVar, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, __vbaRecUniToAnsi, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaUbound, _CIlog, __vbaErrorOverflow, __vbaNew2, __vbaVar2Vec, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarDup, __vbaStrToAnsi, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaUI1Str, __vbaStrMove, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0404 0x04b0
LegalCopyright	Copyright TekSuS
InternalName	GAUFFERED
FileVersion	3.01
CompanyName	TekSuS Silicon
LegalTrademarks	Copyright TekSuS

Description	Data
ProductName	reaving
ProductVersion	3.01
FileDescription	TekSuS Silicon
OriginalFilename	GAUFFERED.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.Trojan.VbCrypt.1981.29338.exe PID: 1364 Parent PID: 5540

General

Start time:	16:20:01
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.VbCrypt.1981.29338.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.VbCrypt.1981.29338.exe'
Imagebase:	0x400000
File size:	136968 bytes
MD5 hash:	41E225BE0600A7EFD31CA3206F97EC17
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis