

ID: 356588
Sample Name:
SecuriteInfo.com.Variant.Razy.845229.20225.25607
Cookbook: default.jbs
Time: 11:49:30
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report SecuriteInfo.com.Variant.Razy.845229.20225.25607 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 4
AV Detection: 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
Entrypoint Preview 10
Data Directories 10
Sections 10
Resources 11
Imports 11
Version Infos 11
Possible Origin 11
Network Behavior 11
Code Manipulations 11
Statistics 11

System Behavior 12
Analysis Process: SecuriteInfo.com.Variant.Razy.845229.20225.exe PID: 7120 Parent PID: 5800 12
General 12
File Activities 12
Disassembly 12
Code Analysis 12

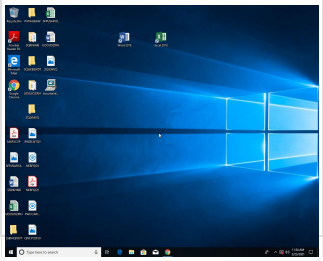
Analysis Report SecuriteInfo.com.Variant.Razy.845229.2…

Overview

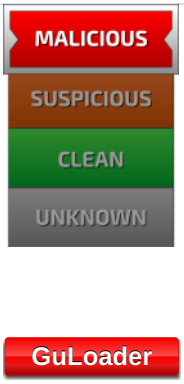
General Information

Sample Name:	SecuriteInfo.com.Variant.Razy.845229.20225.25607 (renamed file extension from 25607 to exe)
Analysis ID:	356588
MD5:	8eb163c0d46881..
SHA1:	6e4efaee511765e.
SHA256:	422cc4ab46ac67…

Most interesting Screenshot:



Detection



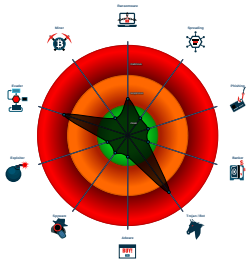
GuLoader

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Detected potential crypto function
- PE file contains an invalid checksum
- PE file contains strange resources
- Program does not show much activi…
- Sample file is different than original …

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Variant.Razy.845229.20225.exe (PID: 7120 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.20225.exe' MD5: 8EB163C0D46881F620662958E37AE6ED)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

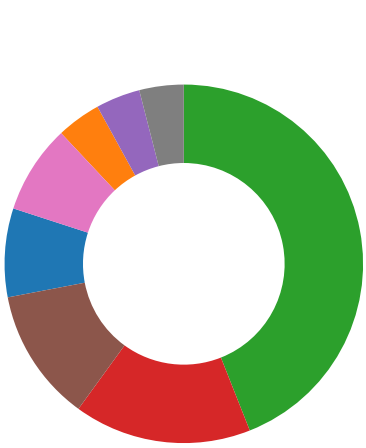
Source	Rule	Description	Author	Strings
Process Memory Space: SecuriteInfo.com.Variant.Razy.845229.20225.exe PID: 7120	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: SecuriteInfo.com.Variant.Razy.845229.20225.exe PID: 7120	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright null 2021



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

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

Anti Debugging:

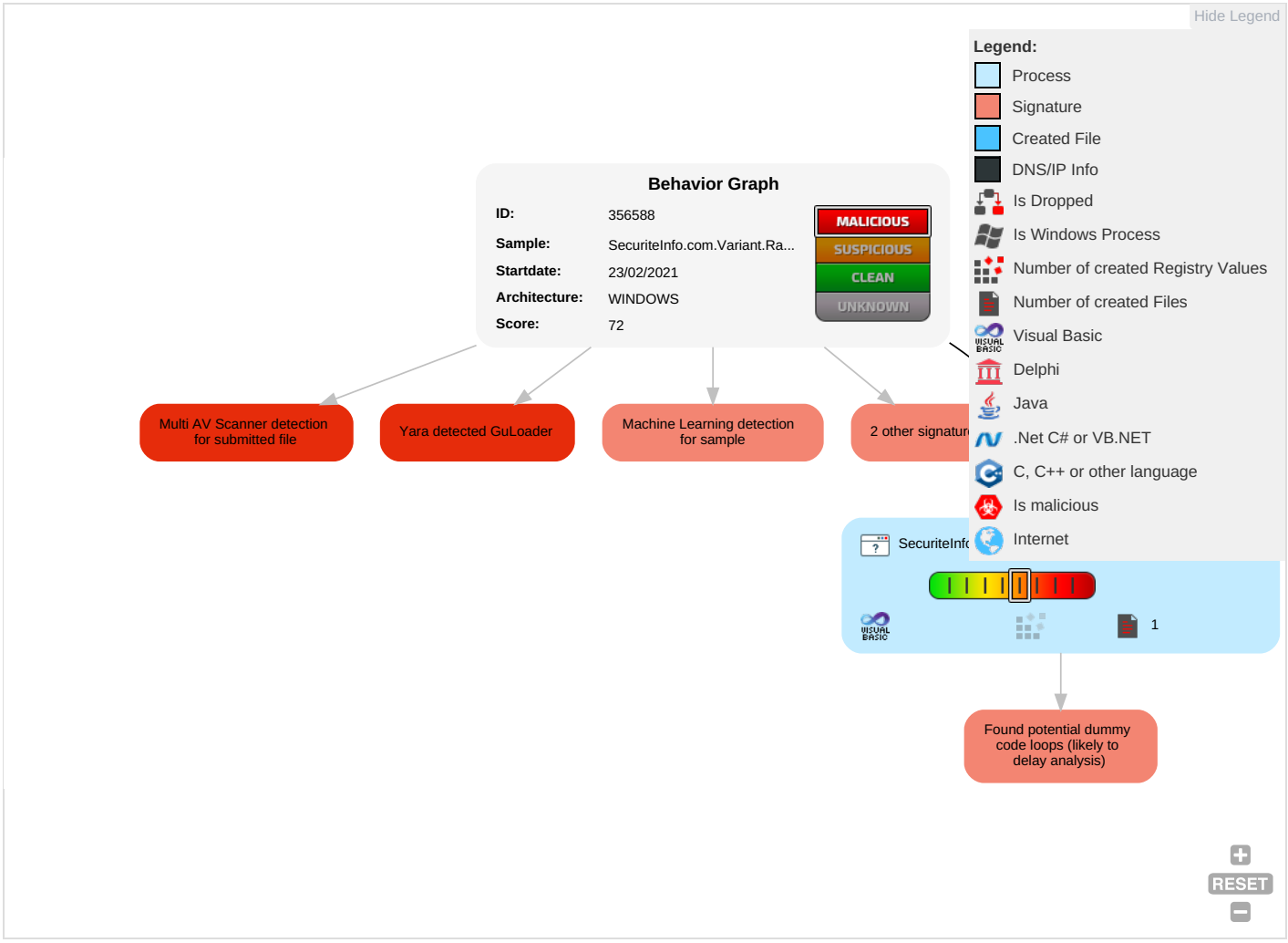
Found potential dummy code loops (likely to delay analysis)

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 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	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 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Copyright null 2021

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.Razy.845229.20225.exe	30%	Virustotal		Browse
SecuriteInfo.com.Variant.Razy.845229.20225.exe	39%	ReversingLabs	Win32.Trojan.Razy	
SecuriteInfo.com.Variant.Razy.845229.20225.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright null 2021

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:	356588
Start date:	23.02.2021
Start time:	11:49:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Razy.845229.20225.25607 (renamed file extension from 25607 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:	15
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:	mal72.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9.9% (good quality ratio 2.3%) • Quality average: 6.6% • Quality standard deviation: 9.6%
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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe

Simulations

Behavior and APIs

Copyright null 2021

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):	5.246218444806131
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.Variant.Razy.845229.20225.exe
File size:	106496
MD5:	8eb163c0d46881f620662958e37ae6ed
SHA1:	6e4efaee511765eeed72eff90ae4eae26b0c162a
SHA256:	422cc4ab46ac67030dcf4da2b6211913c55dbc51962f578a6419ea52417db806
SHA512:	81eaed3574f10ea22841247c9c4ac8fe66787f5f3643e83cfeeca5ee58b408084f4d2420f2bd838879edac9573705184bae2cd768c3e425724d0958b1a6fe029
SSDEEP:	1536:x+g/UQfG5Y4sfIEawyu+EOOKbi/J6d4L+g/UQf:amDfKwlKbi/5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.x.....\...T...%.....Rich.....PE..L....B|N.....@...p.....x.....P....@

File Icon



Icon Hash:	d8d490d4e4bcdae9

Static PE Info

General

Entrypoint:	0x401378
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:	0x4E7C42EA [Fri Sep 23 08:27:22 2011 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:	5fb04c04dc9621084e24b4642ca2fed6

Entrypoint Preview

Instruction
push 004101B8h
call 00007F3FC4872A85h
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 [ecx+457079EFh], ah
int 86h
inc eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x14234	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x18000	0x30a4	.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	0x238	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x114	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Copyright null 2021

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x136fc	0x14000	False	0.340563964844	data	5.78063287873	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x2560	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x18000	0x30a4	0x4000	False	0.10693359375	data	3.24315276856	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x193fc	0x1ca8	data		
RT_ICON	0x18754	0xca8	data		
RT_ICON	0x183ec	0x368	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x183bc	0x30	data		
RT_VERSION	0x18150	0x26c	data	Hungarian	Hungary

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaStrI4, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaLateMemSt, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaVarTstLt, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaVarTstEq, __vbaObjVar, _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, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaVarDup, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x040e 0x04b0
InternalName	punktskatterintrave
FileVersion	1.00
CompanyName	ColdStone
Comments	ColdStone
ProductName	ColdStone
ProductVersion	1.00
OriginalFilename	punktskatterintrave.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Hungarian	Hungary	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: SecuriteInfo.com.Variant.Razy.845229.20225.exe PID: 7120 Parent PID: 5800

General

Start time:	11:50:23
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.20225.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Razy.845229.20225.exe'
Imagebase:	0x400000
File size:	106496 bytes
MD5 hash:	8EB163C0D46881F620662958E37AE6ED
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