ID: 492347
Sample Name:
SecuriteInfo.com.Trojan.BrowseBan.32054.8200
Cookbook: default.jbs
Time: 16:11:05
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.Trojan.BrowseBan.32054.8200 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Analysis Advice 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Jbx Signature Overview 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted IPs 7
General Information 7
Simulations 7
Behavior and APIs 7
Joe Sandbox View / Context 7
IPs 8
Domains 8
ASN 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
Static File Info 8
General 9
File Icon 9
Static PE Info 9
General 9
Entrypoint Preview 9
Data Directories 9
Sections 9
Resources 10
Version Infos 10
Possible Origin 10
Network Behavior 10
Network Port Distribution 10
UDP Packets 10
Code Manipulations 10
Statistics 10
System Behavior 10
Analysis Process: SecuriteInfo.com.Trojan.BrowseBan.32054.exe PID: 4192 Parent PID: 5020 10
General 10
File Activities 11
File Created 11
File Deleted 11
File Written 11
File Read 11
Disassembly 11
Code Analysis 11

Windows Analysis Report SecuriteInfo.com.Trojan.Brow…

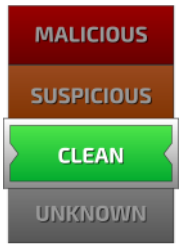
Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.BrowseBan.32054.8200 (renamed file extension from 8200 to exe)
Analysis ID:	492347
MD5:	7a61d4434b4857..
SHA1:	3dc79fb21dc1c58..
SHA256:	44d9fb3b4faeb07..
Tags:	exe
Infos:	

Most interesting Screenshot:

Detection

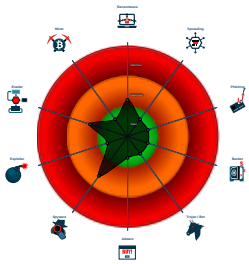


Score:	8
Range:	0 - 100
Whitelisted:	false
Confidence:	40%

Signatures

- Uses 32bit PE files
- PE file does not import any functions
- Queries the volume information (nam…
- PE file contains strange resources
- Tries to load missing DLLs
- Deletes files inside the Windows fold…
- Contains functionality to shutdown / …
- Creates files inside the system direc…
- Detected potential crypto function
- Potential key logger detected (key s…
- Contains functionality to query CPU …
- Contains functionality to retrieve info…
- Contains functionality to check if a w…

Classification



Analysis Advice

Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior

Sample may offer command line options, please run it with the 'Execute binary with arguments' cookbook (it's possible that the command line switches require additional characters like: "-", "/", "--")

Sample has functionality to log and monitor keystrokes, analyze it with the 'Simulates keyboard and window changes' cookbook

Process Tree

- **System is w10x64**
- SecuriteInfo.com.Trojan.BrowseBan.32054.exe (PID: 4192 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.BrowseBan.32054.exe' MD5: 7A61D4434B48575332C6D4227B5ED14F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

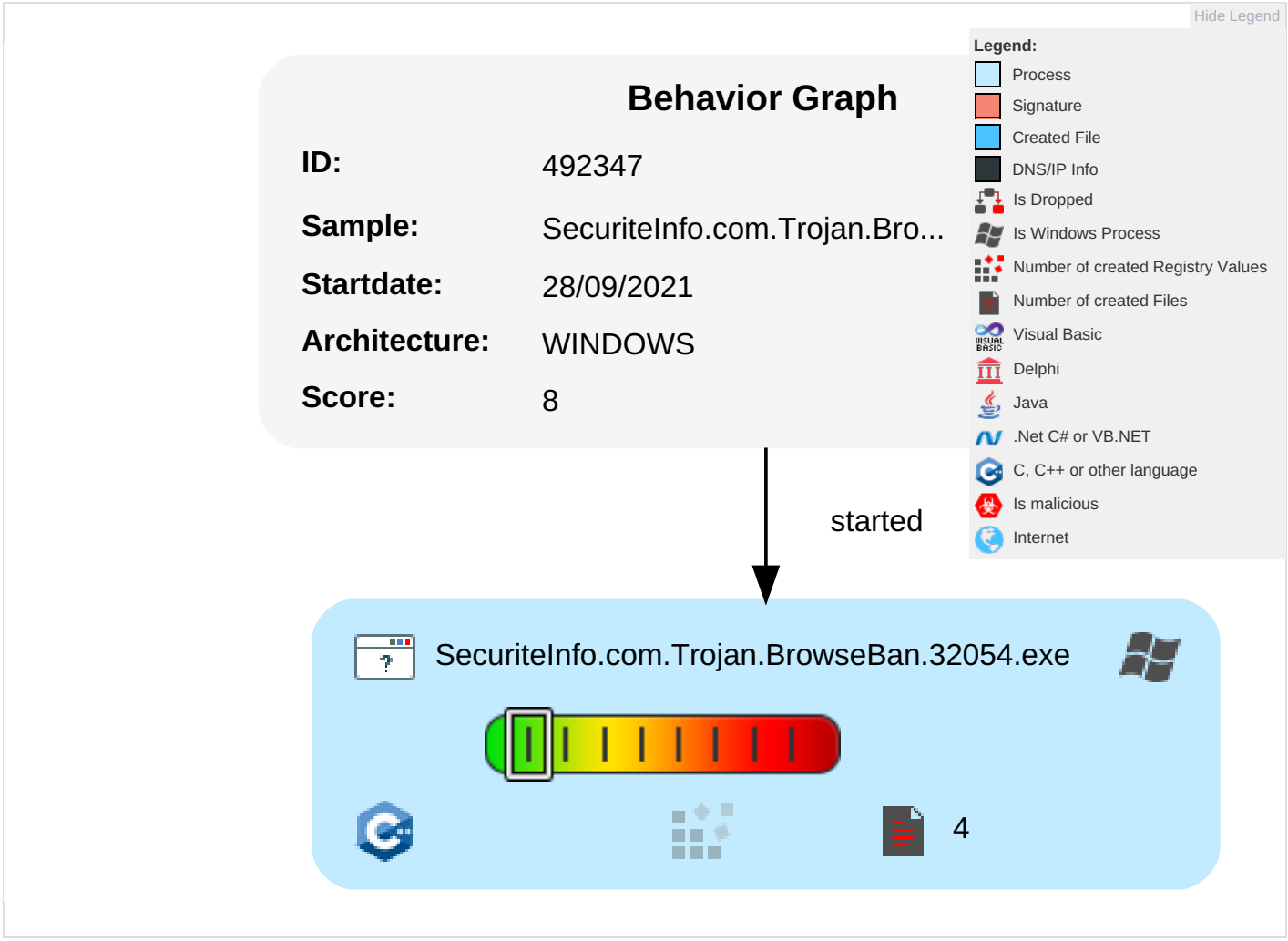
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remo Servi Effec
Valid Accounts	Command and Scripting Interpreter 2	DLL Side-Loading 1	Access Token Manipulation 1	Masquerading 1	Input Capture 2 1	System Time Discovery 1 2	Remote Services	Screen Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remo Track Witho Authe
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Access Token Manipulation 1	LSASS Memory	Application Window Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remo Wipe Witho Authe
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtai Devic Cloud Back
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	File Deletion 1	NTDS	System Information Discovery 2 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

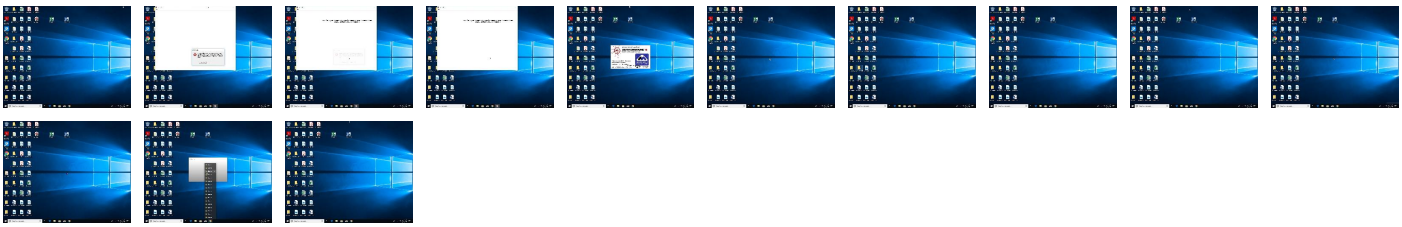
Behavior Graph



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.BrowseBan.32054.exe	3%	Virustotal		Browse
SecuriteInfo.com.Trojan.BrowseBan.32054.exe	5%	Metadefender		Browse
SecuriteInfo.com.Trojan.BrowseBan.32054.exe	2%	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:	33.0.0 White Diamond
Analysis ID:	492347
Start date:	28.09.2021
Start time:	16:11:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.BrowseBan.32054.8200 (renamed file extension from 8200 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:	13
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:	CLEAN
Classification:	clean8.winEXE@1/2@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated
Warnings:	Show All

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

C:\Windows\A6W.INI	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.BrowseBan.32054.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	35
Entropy (8bit):	4.307714802597438
Encrypted:	false
SSDEEP:	3:ExLzdCwpA6jOYp:ENzoLSOI
MD5:	D94D1652055EDF8F49C7991664AFEE1A
SHA1:	97B41753CF7CF84A886E094217BFA850F9D474F8
SHA-256:	6B6D4B0D139E08A0773CF7A591D64DD88825210CE184226423D50DC2BC20F19E
SHA-512:	58B734C2B16339C39ED01B106931AFF9DB41FCEF3435F8E5149F847C028F28C67F171B7711B00242A1BC14C6ED3503F247C01BAFE3184C44F8049ABB91B2EA5E
Malicious:	false
Reputation:	low
Preview:	[MMXTechnology]..MMXEnableCheck=1..

C:\Windows\Run32A60.mch	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.BrowseBan.32054.exe
File Type:	data
Category:	dropped
Size (bytes):	288
Entropy (8bit):	4.686889438956984
Encrypted:	false
SSDEEP:	6:t10rm+aX2qyzwWSXmXlBhMGvqjt/al6wnKfRBm0opzlLNlv8uFRxjw3:707H02XkR0LXphNlv8uFg3
MD5:	DDBD22FCBC5FC8DD7E120DBF85CA9519
SHA1:	877C624A1829038173D8BF1B898ABA3EDD99BF81
SHA-256:	E0C5778E7BFEC2EB403609850616FFA2ADD712AED5616D5B1F6891B99C6CB8F3
SHA-512:	F699679FEAC9364186BEEA2FBEAC3541F44280BD42FF3A716F384EBE27AAF2674858F86941CF2F756EAB28E13DDC18F83999F42A0CC802A0D09666D65DB9DF9B
Malicious:	false
Reputation:	low
Preview:	MoaCacheWin32_32.....OsType.....XtraClassInfo.....DirSpec....._rt_KeepInCache.....AlwaysCallRegister....._rt_RegDictList.....FileName....._rt_XtraDictList....._rt_XtraRef....._rt_FileDictList....._rt_NeedsRegistration.....Date.....FileHasXtraEntriesAdded.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.267914993120473
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Trojan.BrowseBan.32054.exe
File size:	1570477
MD5:	7a61d4434b48575332c6d4227b5ed14f
SHA1:	3dc79fb21dc1c58a3f9fb3fd5a94b5a4eb5cfd36
SHA256:	44d9fb3b4faeb07506a95eaf45e7d9d40dac2830f2004bb6ca061167aa9a67e4
SHA512:	f51b4a93a2aebdbe89dc31d53363497d9d50cc178c530b7a25c0baa9770e01e7430ceb4365034e4fc6209aa3411e6b1d4fa4f79184f0de3735956278943dc668
SSDEEP:	24576:rjGjEneWcf3c+rkqPGIwLqyz6phJLxwpX16ON/+vxM1fVQLcmOZ4WM7:fGnf3wOl0HgMpVQLMZM7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....c.;.....@.....@.....5..

File Icon

Icon Hash:	f2ecd4b2f6f4c4ec

Static PE Info

General

Entrypoint:	0x4f1340
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:	
Time Stamp:	0x3B8363CE [Wed Aug 22 07:48:30 2001 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:	

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xfb3f6	0xfb400	False	0.512184196206	data	6.37515393741	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xfd000	0x3015	0x3200	False	0.435078125	data	5.40448218626	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x101000	0xd074	0x5e00	False	0.400556848404	data	4.46430466957	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.idata	0x10f000	0x28f8	0x2a00	False	0.407087053571	data	5.53322081171	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x112000	0x5c490	0x5c600	False	0.179288417625	data	4.12178722438	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x16f000	0xba6a	0xbc00	False	0.625020777926	data	6.2745480459	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.BrowseBan.32054.exe PID: 4192 Parent PID: 5020

General

Start time:	16:12:02
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.BrowseBan.32054.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.BrowseBan.32054.exe'
Imagebase:	0x400000
File size:	1570477 bytes
MD5 hash:	7A61D4434B48575332C6D4227B5ED14F
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis