ID: 404310
Sample Name:
SecuriteInfo.com.Trojan.GenericKD.46243806.32106.30285
Cookbook: default.jbs
Time: 22:10:56
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

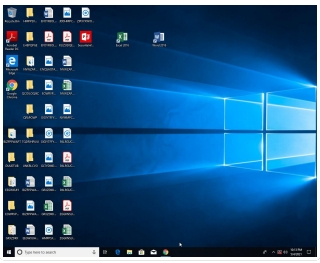
Analysis Report SecuriteInfo.com.Trojan.GenericKD.462…

Overview

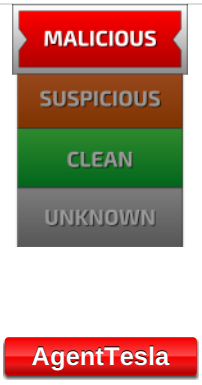
General Information

Sample Name:	SecuriteInfo.com.Trojan.GenericKD.46243806.32106.30285 (renamed file extension from 30285 to exe)
Analysis ID:	404310
MD5:	cce6c363c0ff7ac…
SHA1:	98ad5e24bf99fbb..
SHA256:	b65eed317058df5.
Infos:	

Most interesting Screenshot:



Detection

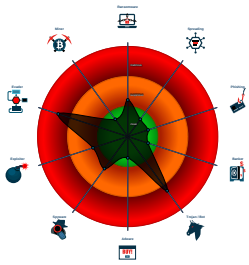


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Creates an undocumented autostart …
- Injects a PE file into a foreign proce…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Writes to foreign memory regions
- Abnormal high CPU Usage
- Antivirus or Machine Learning detec…
- Contains long sleeps (>= 3 min)
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe (PID: 5968 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe' MD5: CCE6C363C0FF7AC663CD71C5906069A6)
  - SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe (PID: 2044 cmdline: C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe MD5: CCE6C363C0FF7AC663CD71C5906069A6)
  - SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe (PID: 1848 cmdline: C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe MD5: CCE6C363C0FF7AC663CD71C5906069A6)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "bigazz@sixjan.xyzH^i?T2&gWQ({sixjan.xyz"
}
```

Yara Overview

Memory Dumps

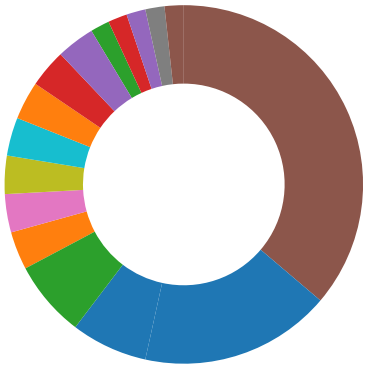
Source	Rule	Description	Author	Strings
00000010.00000002.484888113.0000000002BB1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000010.00000002.484888113.0000000002BB1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe PID: 1848	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe PID: 1848	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Boot Survival:

Creates an undocumented autostart registry key

Malware Analysis System Evasion:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

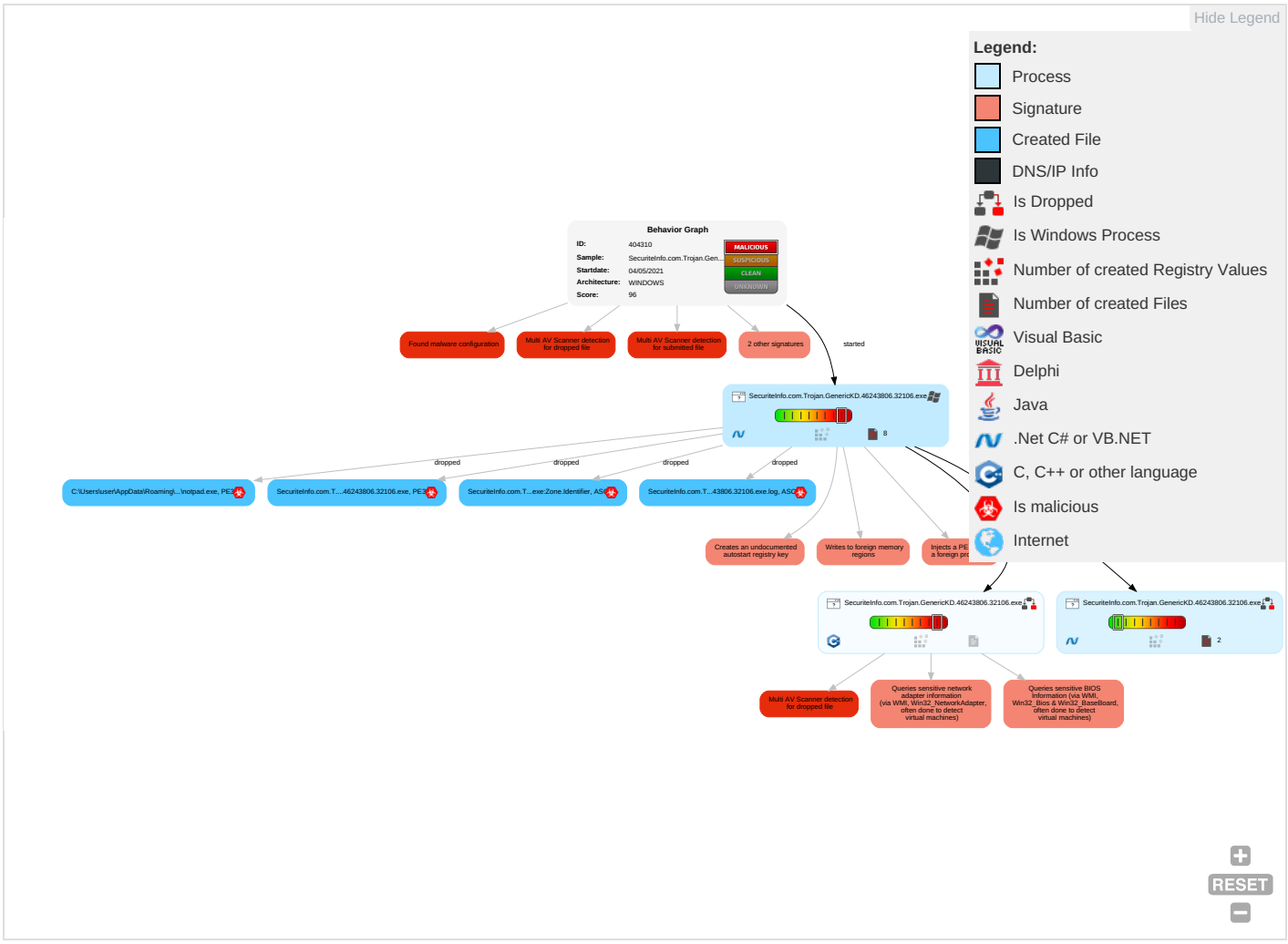
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	E
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1 1	Process Injection 2 1 2	Masquerading 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E I N C
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 3 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	E F C
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	N D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 3	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S

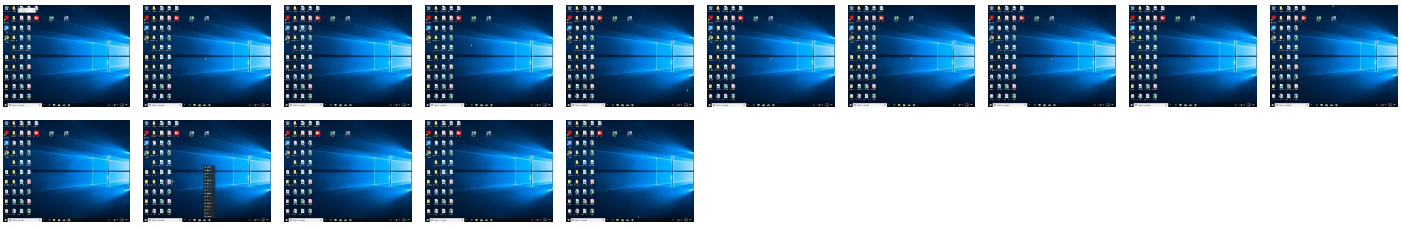
Behavior Graph



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.46243806.32106.exe	31%	Virustotal		Browse
SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe	40%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe	40%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad\notpad.exe	40%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe.428c788.2.unpack	100%	Avira	HEUR/AGEN.1110362		Download File
16.2.SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe.432c7a8.3.unpack	100%	Avira	HEUR/AGEN.1110362		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://discord.com/2	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/6	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://mNVnNH.com	0%	Avira URL Cloud	safe	
http://https://discord.com/:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe, 00000010.00000002.484888113.0000000002BB1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org%GETMozilla/5.0	SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe, 00000010.00000002.484888113.0000000002BB1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://discord.com/2	SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe, 00000010.00000002.484888113.0000000002BB1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://discord.com/	SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://discord.com/6	SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe, 00000010.00000002.484888113.0000000002BB1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mNVnNH.com	SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe, 00000010.00000002.484888113.0000000002BB1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://discord.com/:	SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404310
Start date:	04.05.2021
Start time:	22:10:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.GenericKD.46243806.32106.30285 (renamed file extension from 30285 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:	27
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:	mal96.troj.evad.winEXE@5/5@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 62.5% • Quality standard deviation: 14.5%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:13:06	API Interceptor	359x Sleep call for process: SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad\notpad.exe	IMG_05412_868_21.docx	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe	IMG_05412_868_21.docx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	697
Entropy (8bit):	5.329165082425189
Encrypted:	false
SSDEEP:	12:Q3La/hzzAbDLI4M9tDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9l0ZKhat/DLI4M/DD:MLasXE4qpE4Ks2wKDE4KhK3VZ9pKhgLU
MD5:	0832DF9444C16D83CFAAE29AC72D03D6
SHA1:	AA245EF747FBA8996C83FC74147657D51467C058
SHA-256:	5039464C89038FB81B6DFF61330D29D31630C393AB578CDEC6628699E8906C76
SHA-512:	5C2F08CFC35E6579972E20C9241313B52B89D419B8EE0C51E248AFC094B3C816B09427E4806C5DDD0E050C3AC24ACB61CD2E8D78415BCEF01491F2D6FC8FFD4
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	343352
Entropy (8bit):	7.841371992370745
Encrypted:	false
SSDEEP:	6144:FL4Qez8X+5KBrIxuNWUwJm4OdB17ZDs0s7xHAVkYifH4TWcwb8tFHQK:V4Qez+YSSjUAmdr17Zw0+geYqH41wb88
MD5:	CCE6C363C0FF7AC663CD71C5906069A6
SHA1:	98AD5E24BF99FBB4CF7BDCAA54B6D720064DC810
SHA-256:	B65EED317058DF5DDD4247EC93AC2B555AE2C29B751EE455CEEE3DD9B670ECAD
SHA-512:	C3E28465D1FB8673D4B203D3A985AF370255E1381EA8D9DB910F213EFFC4F5C3CA0214497FA783396A25C4316D5CDDE6F05A35BBF44581EF5BC4C2FCD4F8FAB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 40%

C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe	
Joe Sandbox View:	• Filename: IMG_05412_868_21.docx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H..`.....J.....^... .....@.. ..... ..@.....K.....,G.....8....`..... ....H.....text...d.... ....`.rsrc...,G.....H.....@..@.rel oc.....`.....@..B.....@.....H.....J..$,.....w...y.....0.....:.....(/...8....&.....(.....s....o.... .>n.(5....:6...& .>n.(5.....%.(- .....!...&& a>n.(5...('...&8....((...8....(*...8....*.....0.....(.....(....o.... ^>n.(5...(....o....:....&8.....8....s.....:....&..o....o....s....9....&8.....8....8....s.....s....s.....o.....o .....o.....o.....o.....(.....o.....9.....o.....*.4.....

C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad\notpad.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	343352
Entropy (8bit):	7.841371992370745
Encrypted:	false
SSDEEP:	6144:FL4Qez8X+5KBrIxuNWUwJm4OdB17ZDs0s7xHAVkYifH4TWcwb8tFHQK:V4Qez+YSSjUAmdr17Zw0+geYqH41wb88
MD5:	CCE6C363C0FF7AC663CD71C5906069A6
SHA1:	98AD5E24BF99FBB4CF7BDCAA54B6D720064DC810
SHA-256:	B65EED317058DF5DDD4247EC93AC2B555AE2C29B751EE455CEEE3DD9B670ECAD
SHA-512:	C3E28465D1FB8673D4B203D3A985AF370255E1381EA8D9DB910F213EFFC4F5C3CA0214497FA783396A25C4316D5CDDE6F05A35BBF44581EF5BC4C2FCD4F8FAB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 40%
Joe Sandbox View:	• Filename: IMG_05412_868_21.docx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H..`.....J.....^... .....@.. ..... ..@.....K.....,G.....8....`..... ....H.....text...d.... ....`.rsrc...,G.....H.....@..@.rel oc.....`.....@..B.....@.....H.....J..$,.....w...y.....0.....:.....(/...8....&.....(.....s....o.... .>n.(5....:6...& .>n.(5.....%.(- .....!...&& a>n.(5...('...&8....((...8....(*...8....*.....0.....(.....(....o.... ^>n.(5...(....o....:....&8.....8....s.....:....&..o....o....s....9....&8.....8....8....s.....s....s.....o.....o .....o.....o.....o.....(.....o.....9.....o.....*.4.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad\notpad.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.841371992370745
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe
File size:	343352
MD5:	cce6c363c0ff7ac663cd71c5906069a6
SHA1:	98ad5e24bf99fbb4cf7bdcaa54b6d720064dc810
SHA256:	b65eed317058df5ddd4247ec93ac2b555ae2c29b751ee455ceee3dd9b670ecad
SHA512:	c3e28465d1fb8673d4b203d3a985af370255e1381ea8d9cb910f213effc4f5c3ca0214497fa783396a25c4316d5cdde6f05a35bbf44581ef5bc4c2fcd4f8fa1b
SSDEEP:	6144:FL4Qez8X+5KBrlxuNWUwJm4OdB17ZDs0s7xHAVkYifH4TWcwb8tFHQK:V4Qez+YSSjUAmdr17Zw0+geYqH41wb88
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...H..`.....J.....^.... .....@.. .....@.....

File Icon

Icon Hash:	0378d8d6dad83047

Static PE Info

General

Entrypoint:	0x44f05e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60908048 [Mon May 3 22:59:20 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert EV Code Signing CA (SHA2), OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 3/13/2018 5:00:00 PM 2/18/2021 4:00:00 AM

Subject Chain	• CN=Discord Inc., O=Discord Inc., L=San Francisco, S=California, C=US, SERIALNUMBER=5128862, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US
Version:	3
Thumbprint MD5:	831AE83D7C56E51AE513F0ED5D99DC4E
Thumbprint SHA-1:	1E6706B746A7409F4E9A39855C5DDE4155A13056
Thumbprint SHA-256:	584035E0344227FC32C92A7F3FD4D88594A26C2E953360543D613329E99122DD
Serial:	04F131322CC31D92C849FCA351D2F141

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4f010	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x50000	0x472c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x51e00	0x1f38	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x56000	0xc	.reloc
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	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	0x4d064	0x4d200	False	0.96637902654	data	7.96408240927	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x50000	0x472c	0x4800	False	0.0664605034722	data	2.1900964107	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x56000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x50130	0x4028	data		
RT_GROUP_ICON	0x54158	0x14	data		
RT_VERSION	0x5416c	0x40a	data		
RT_MANIFEST	0x54578	0x1b4	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright (c) 2020 Discord Inc. All rights reserved.
Assembly Version	0.0.52.0
InternalName	44444.exe
FileVersion	0.0.52.0
CompanyName	Discord Inc.
LegalTrademarks	
Comments	Discord - https://discord.com/
ProductName	Discord - https://discord.com/
ProductVersion	0.0.52.0
FileDescription	Discord - https://discord.com/
OriginalFilename	44444.exe

Network Behavior

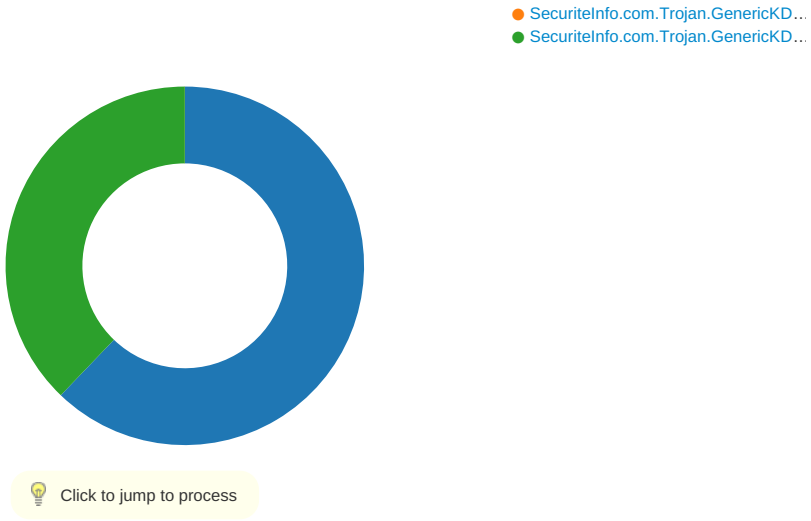
No network behavior found

Code Manipulations

Statistics

Behavior

● SecuriteInfo.com.Trojan.GenericKD…



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe PID: 5968
Parent PID: 5600

General

Start time:	22:11:51
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe'
Imagebase:	0xc20000
File size:	343352 bytes
MD5 hash:	CCE6C363C0FF7AC663CD71C5906069A6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6DFFCF06	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	6DFFCF06	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE4BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad\notpad.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	5FA51A3	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad\notpad.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	5FA51A3	CopyFileW
C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	5FA51A3	CopyFileW
C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	5FA51A3	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E30C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad\notpad.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 48 80 90 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 d2 04 00 00 4a 00 00 00 00 00 00 5e f0 04 00 00 20 00 00 00 00 05 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 05 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...H..`.......... ....J......^.... ....@.. ....@................	success or wait	3	5FA51A3	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad\notpad.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	5FA51A3	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 48 80 90 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 d2 04 00 00 4a 00 00 00 00 00 00 5e f0 04 00 00 20 00 00 00 00 05 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 05 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...H..`.......... ....J......^.... ....@.. ....@................	success or wait	3	5FA51A3	CopyFileW
C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	5FA51A3	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe.log	unknown	697	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 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 34 2e 30 2e 33 30 33 31	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3031	success or wait	1	6E30C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Startup	unicode	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad	success or wait	1	6CE4646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Startup	unicode	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notpad	success or wait	1	6CE4646A	RegSetValueExW

Analysis Process: SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe PID: 2044
Parent PID: 5968

General

Start time:	22:12:48
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe
Imagebase:	0x230000
File size:	343352 bytes
MD5 hash:	CCE6C363C0FF7AC663CD71C5906069A6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 40%, ReversingLabs
Reputation:	low

Analysis Process: SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe PID: 1848
Parent PID: 5968

General

Start time:	22:12:49
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\SecuriteInfo.com.Trojan.GenericKD.46243806.32106.exe
Imagebase:	0x6e0000
File size:	343352 bytes
MD5 hash:	CCE6C363C0FF7AC663CD71C5906069A6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.484888113.0000000002BB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.484888113.0000000002BB1000.00000004.00000001.sdmp, Author: Joe Security
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	6DFFCF06	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	6DFFCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile

Disassembly

Code Analysis