ID: 502297
Sample Name:
SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.27244
Cookbook: default.jbs
Time: 19:27:08
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

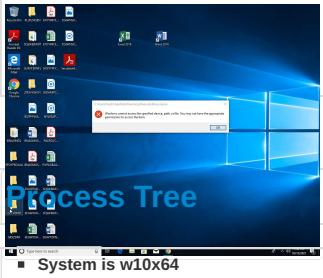
Windows Analysis Report SecuriteInfo.com.BackDoor.S…

Overview

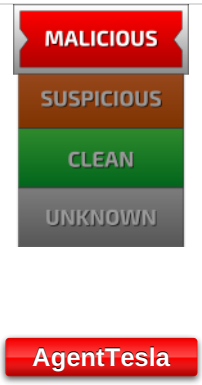
General Information

Sample Name:	SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.27244 (renamed file extension from 27244 to exe)
Analysis ID:	502297
MD5:	a665b705b9381b..
SHA1:	a6fba4f009921b1..
SHA256:	dc07322ef165269.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

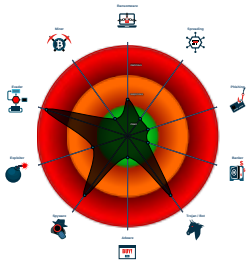


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Hides that the sample has been dow…
- Tries to steal Mail credentials (via fil…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…

Classification



- **System is w10x64**
- SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe (PID: 4608 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe' MD5: A665B705B9381B33AAA9E307FE340AF7)
  - SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe (PID: 5252 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe MD5: A665B705B9381B33AAA9E307FE340AF7)
- BnevyAj.exe (PID: 5328 cmdline: 'C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe' MD5: A665B705B9381B33AAA9E307FE340AF7)
  - BnevyAj.exe (PID: 5476 cmdline: C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe MD5: A665B705B9381B33AAA9E307FE340AF7)
- BnevyAj.exe (PID: 7036 cmdline: 'C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe' MD5: A665B705B9381B33AAA9E307FE340AF7)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "info@croatiahunt.com",
  "Password": "VilaVrgade852",
  "Host": "mail.croatiahunt.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.571975885.0000000002F51000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.571975885.0000000002F51000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.339779218.000000000030E1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.340326707.00000000040E9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.340326707.00000000040E9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.BnevyAj.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.2.BnevyAj.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.2.SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe.428bd80.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 17 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Tries to harvest and steal browser information (history, passwords, etc)

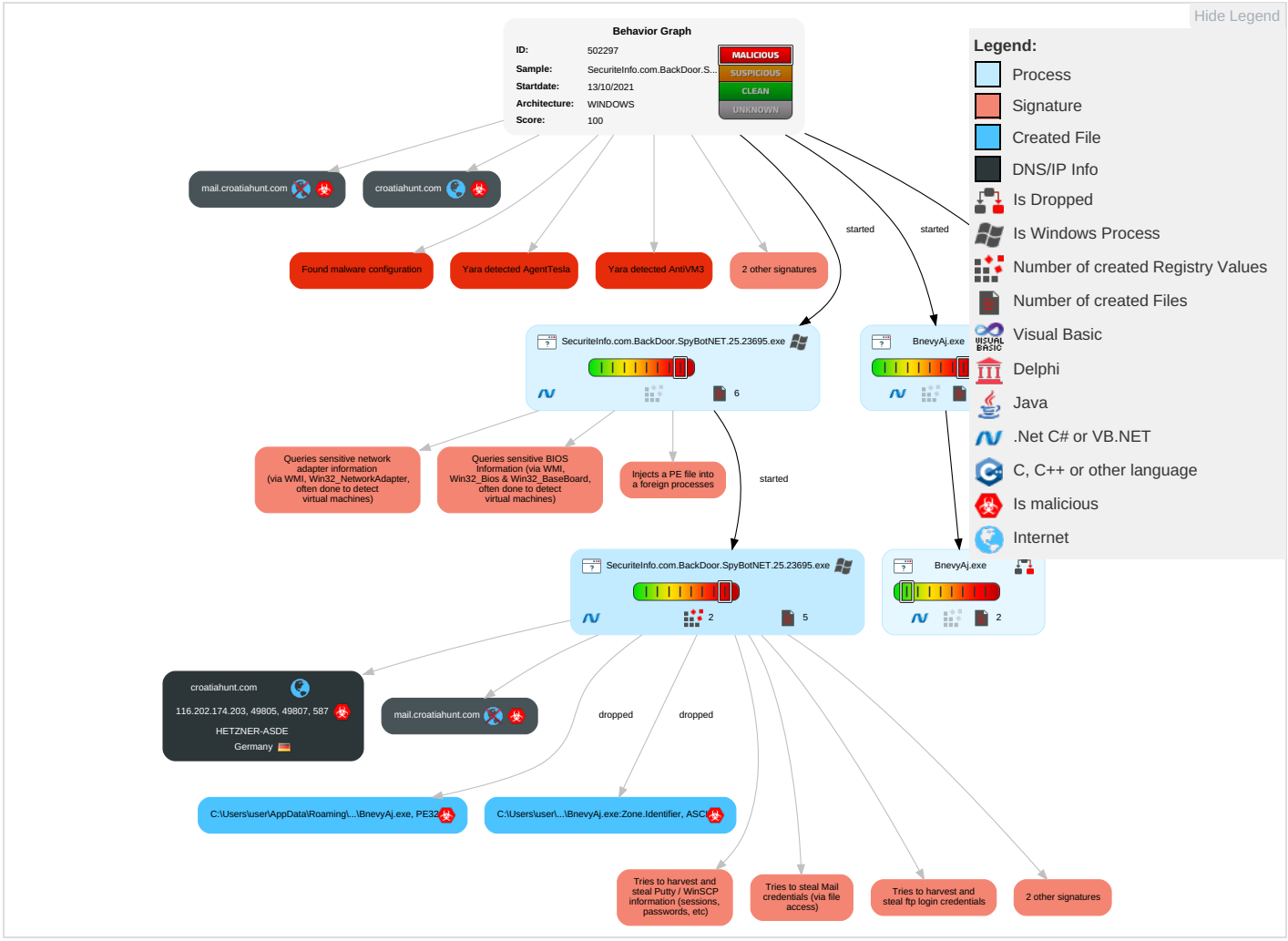
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 2 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	Credentials in Registry 1	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

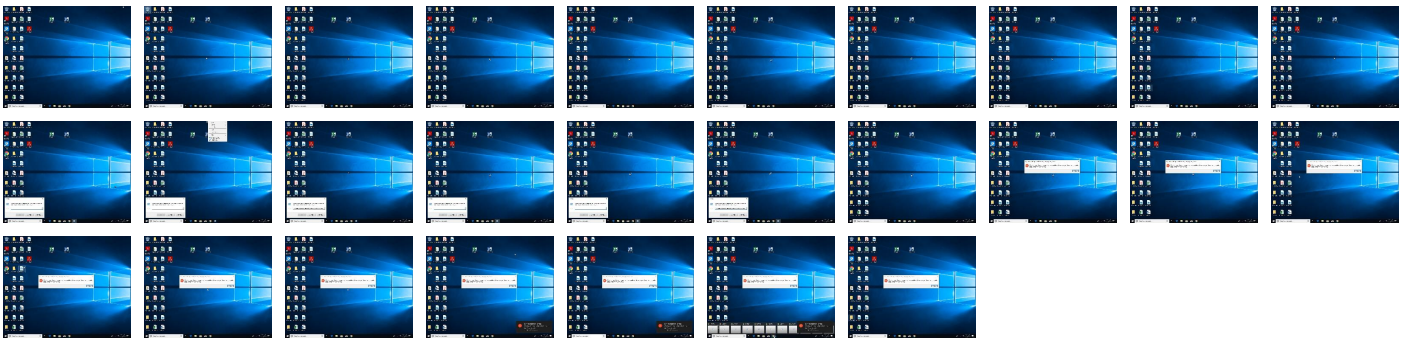
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.BnevyAj.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.2.SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.com5	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://vF9HSjffwxoWNFAu.org	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnA	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.comF	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/7	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/-cz	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.fontbureau.comion%	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://MpOtQG.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnj	0%	URL Reputation	safe	
http://www.fonts.comyp	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comY	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.krll	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://mail.croatiahunt.com	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	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://www.fonts.comn-u	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://en.w$	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/alik	0%	Avira URL Cloud	safe	
http://fontfabrik.com7	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://croatiahunt.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fonts.com8	0%	URL Reputation	safe	
http://www.sandoll.co.krre	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
croatiahunt.com	116.202.174.203	true	true		unknown
mail.croatiahunt.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
116.202.174.203	croatiahunt.com	Germany		24940	HETZNER-ASDE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502297
Start date:	13.10.2021
Start time:	19:27:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.27244 (renamed file extension from 27244 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:	22
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:	mal100.troj.spyw.evad.winEXE@7/4@4/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 16% • Quality standard deviation: 25.3%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:28:25	API Interceptor	668x Sleep call for process: SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe modified
19:28:54	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run BnevyAj C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe
19:29:02	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run BnevyAj C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe
19:29:08	API Interceptor	405x Sleep call for process: BnevyAj.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
116.202.174.203	DHL consignment number_600595460.xlsx	Get hash	malicious	Browse	
	Po____211110.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	FTdhc25gn8.exe	Get hash	malicious	Browse	• 88.99.75.82
	SecuriteInfo.com.Ransom.Stop.Z5.27157.exe	Get hash	malicious	Browse	• 88.99.75.82
	Ref 0180066743.xlsx	Get hash	malicious	Browse	• 136.243.159.53
	DHL consignment number_600595460.xlsx	Get hash	malicious	Browse	• 116.202.174.203
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 88.99.66.31
	HqiJ8HpbxU.exe	Get hash	malicious	Browse	• 136.243.159.53
	zrArDsoum0.exe	Get hash	malicious	Browse	• 88.99.75.82
	0000000588.pdf.exe	Get hash	malicious	Browse	• 116.203.31.151
	FAj7shxXukkNrTk.exe	Get hash	malicious	Browse	• 88.99.137.80
	UZWdHg3hWA.exe	Get hash	malicious	Browse	• 88.99.75.82
	LBJiq1QBaH.exe	Get hash	malicious	Browse	• 88.99.75.82
	NZi63BWERD.exe	Get hash	malicious	Browse	• 168.119.93.163
	3ZDXaih2Iv.exe	Get hash	malicious	Browse	• 5.9.250.2
	y5V9T1zkVO.exe	Get hash	malicious	Browse	• 136.243.159.53
	p6fx0L15Ae.exe	Get hash	malicious	Browse	• 168.119.93.163
	SecuriteInfo.com.PUA.Tool.Linux.BtcMine.2805.26628.5655	Get hash	malicious	Browse	• 88.99.193.240
	Purchase_order_21518.doc	Get hash	malicious	Browse	• 95.216.94.72
	Order EQE0905.xlsx	Get hash	malicious	Browse	• 168.119.93.163
	Contract.xlsx	Get hash	malicious	Browse	• 136.243.159.53
	SwiftRefINV0899211.xlsx	Get hash	malicious	Browse	• 136.243.159.53

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe	DHL consignment number_600595460.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BnevyAj.exe.log	
Process:	C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.348115897127242
Encrypted:	false
SSDEEP:	24:MLUE4KJXE4qpE4Ks2E1qE4qpAE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4x88:MIHKtH2HKXE1qHmAHKzvRYHKhQnoPtH2
MD5:	832D6A22CE7798D72609B9C21B4AF152
SHA1:	B086DE927BFEE6039F5555CE53C397D1E59B4CA4
SHA-256:	9E5EE72EF293C66406AF155572BF3B0CF9DA09CC1F60ED6524AAFD65553CE551
SHA-512:	A1A70F76B98C2478830AE737B4F12507D859365F046C5A415E1EBE3D87FFD2B64663A31E1E5142F7C3A7FE9A6A9CB8C143C2E16E94C3DD6041D1CCABEDDD2C21
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BnevyAj.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Deployment, 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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.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..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.348115897127242
Encrypted:	false
SSDEEP:	24:MLUE4KJXE4qpE4Ks2E1qE4qpAE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4x88:MIHKtH2HKXE1qHmAHKzvRYHKhQnoPtH2
MD5:	832D6A22CE7798D72609B9C21B4AF152
SHA1:	B086DE927BFEE6039F5555CE53C397D1E59B4CA4
SHA-256:	9E5EE72EF293C66406AF155572BF3B0CF9DA09CC1F60ED6524AAFD65553CE551
SHA-512:	A1A70F76B98C2478830AE737B4F12507D859365F046C5A415E1EBE3D87FFD2B64663A31E1E5142F7C3A7FE9A6A9CB8C143C2E16E94C3DD6041D1CCABEDDD2C21
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Deployment, 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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.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..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows

C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	564736
Entropy (8bit):	7.0819561487133305
Encrypted:	false
SSDEEP:	6144:0MkhBXuLbabNr+o6RxQbACvuj8qLhT7uu5ziEjPY2hL1Vkebv0duOjwYB:vSBXuLbalbMebAr9LNu3KY8L1u+0j1
MD5:	A665B705B9381B33AAA9E307FE340AF7
SHA1:	A6FBA4F009921B1DE9D524047BCB7FA0E571A116
SHA-256:	DC07322EF1652695B5E85BFD5D6DA8C5B6C311D26FF13EB18A390CD4B7232203
SHA-512:	B7E7FF96DCE12935C71B6E6B6FC74652CD08725D8DE29A91E35B0D4F8F351D14F371E2D48A3AB5FE733003764AF09B6BE6DC6D943112B596FA2B09A7638BBAE
Malicious:	**true**
Joe Sandbox View:	• Filename: DHL consignment number_600595460.xlsx, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...S.fa.....0..(...t.....RF... ...`....@.. ..@.....F..O...`..(q..... ....H.....text...X&... ...(..... ..`.rsrc...(q...`...r...*.....@..@.relococ.....@..B.....4F.....H.....Lb...O.....Y...`.....0..V.....}.....*.*s....}.....}.....}.....(.....(.....{....r...po.....{....r...po.....*...0.....(....&.{.....,....8....sA...%.{....|....(....Z.{....|....(....Z . &.s....} ...%.}.....{ ...(.....(....o.....+c...+C.....X.}.....,+..(.....{....Z...{....Z.{....{....o .....X.....|....(.....-....X.....|....(.....-.....,..o!.....sB.....|....(.....|....(....s"

C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.0819561487133305
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe
File size:	564736
MD5:	a665b705b9381b33aaa9e307fe340af7
SHA1:	a6fba4f009921b1de9d524047bcb7fa0e571a116
SHA256:	dc07322ef1652695b5e85bfd5d6da8c5b6c311d26ff13eb18a390cd4b7232203
SHA512:	b7e7ff96dce12935c71b6e6b6fc74652cd08725d8de29a91e35b0d4f8f351d14f371e2d48a3ab5fe733003764af09b6be6dc6d943112b596fa2b09a7638bbaee
SSDEEP:	6144:0MkhBXuLbabNr+o6RxQbACvuj8qLhT7uu5ziEjPY2hL1Vkebv0duOjwYB:vSBXuLbalbMebAr9LNu3KY8L1u+0j1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...S.fa.....0..(...t.....RF... ...`....@.. .....@.....

File Icon

Icon Hash:	0c529252d9cce41b

Static PE Info

General

Entrypoint:	0x464652
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61668753 [Wed Oct 13 07:14:27 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

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x62658	0x62800	False	0.889331178617	data	7.80231606159	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x66000	0x27128	0x27200	False	0.141298921725	data	3.94408724321	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 19:30:12.850055933 CEST	192.168.2.3	8.8.8.8	0x7973	Standard query (0)	mail.croatiahunt.com	A (IP address)	IN (0x0001)
Oct 13, 2021 19:30:12.927783012 CEST	192.168.2.3	8.8.8.8	0x9dd6	Standard query (0)	mail.croatiahunt.com	A (IP address)	IN (0x0001)
Oct 13, 2021 19:30:38.734894037 CEST	192.168.2.3	8.8.8.8	0xb93d	Standard query (0)	mail.croatiahunt.com	A (IP address)	IN (0x0001)
Oct 13, 2021 19:30:38.756289005 CEST	192.168.2.3	8.8.8.8	0xdf3b	Standard query (0)	mail.croatiahunt.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 19:30:12.875040054 CEST	8.8.8.8	192.168.2.3	0x7973	No error (0)	mail.croatiahunt.com	croatiahunt.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 19:30:12.875040054 CEST	8.8.8.8	192.168.2.3	0x7973	No error (0)	croatiahunt.com		116.202.174.203	A (IP address)	IN (0x0001)
Oct 13, 2021 19:30:12.954381943 CEST	8.8.8.8	192.168.2.3	0x9dd6	No error (0)	mail.croatiahunt.com	croatiahunt.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 19:30:12.954381943 CEST	8.8.8.8	192.168.2.3	0x9dd6	No error (0)	croatiahunt.com		116.202.174.203	A (IP address)	IN (0x0001)
Oct 13, 2021 19:30:38.753648996 CEST	8.8.8.8	192.168.2.3	0xb93d	No error (0)	mail.croatiahunt.com	croatiahunt.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 19:30:38.753648996 CEST	8.8.8.8	192.168.2.3	0xb93d	No error (0)	croatiahunt.com		116.202.174.203	A (IP address)	IN (0x0001)
Oct 13, 2021 19:30:38.774570942 CEST	8.8.8.8	192.168.2.3	0xdf3b	No error (0)	mail.croatiahunt.com	croatiahunt.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 19:30:38.774570942 CEST	8.8.8.8	192.168.2.3	0xdf3b	No error (0)	croatiahunt.com		116.202.174.203	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Oct 13, 2021 19:30:15.159970999 CEST	587	49805	116.202.174.203	192.168.2.3	220-srv1.kuhada.com ESMTP Exim 4.94.2 #2 Wed, 13 Oct 2021 19:30:15 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Oct 13, 2021 19:30:15.160794973 CEST	49805	587	192.168.2.3	116.202.174.203	EHLO 061544
Oct 13, 2021 19:30:15.182768106 CEST	587	49805	116.202.174.203	192.168.2.3	250-srv1.kuhada.com Hello 061544 [102.129.143.33] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Oct 13, 2021 19:30:15.183624983 CEST	49805	587	192.168.2.3	116.202.174.203	STARTTLS
Oct 13, 2021 19:30:15.207288980 CEST	587	49805	116.202.174.203	192.168.2.3	220 TLS go ahead
Oct 13, 2021 19:30:38.822663069 CEST	587	49807	116.202.174.203	192.168.2.3	220-srv1.kuhada.com ESMTP Exim 4.94.2 #2 Wed, 13 Oct 2021 19:30:38 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Oct 13, 2021 19:30:38.823153019 CEST	49807	587	192.168.2.3	116.202.174.203	EHLO 061544
Oct 13, 2021 19:30:38.844769955 CEST	587	49807	116.202.174.203	192.168.2.3	250-srv1.kuhada.com Hello 061544 [102.129.143.33] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Oct 13, 2021 19:30:38.845032930 CEST	49807	587	192.168.2.3	116.202.174.203	STARTTLS
Oct 13, 2021 19:30:38.867923975 CEST	587	49807	116.202.174.203	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe PID: 4608
Parent PID: 3876

General

Start time:	19:28:10
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe'
Imagebase:	0xe00000
File size:	564736 bytes
MD5 hash:	A665B705B9381B33AAA9E307FE340AF7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.339779218.00000000030E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.340326707.00000000040E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.340326707.00000000040E9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe PID: 5252 Parent PID: 4608

General

Start time:	19:28:26
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.BackDoor.SpyBotNET.25.23695.exe
Imagebase:	0xbc0000
File size:	564736 bytes
MD5 hash:	A665B705B9381B33AAA9E307FE340AF7
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: 00000004.00000002.571975885.0000000002F51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.571975885.0000000002F51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.568503526.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.568503526.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: BnevyAj.exe PID: 5328 Parent PID: 3352

General

Start time:	19:29:02
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe'
Imagebase:	0x1c0000
File size:	564736 bytes
MD5 hash:	A665B705B9381B33AAA9E307FE340AF7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.427226592.0000000002541000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.427794658.0000000003549000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000002.427794658.0000000003549000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: BnevyAj.exe PID: 5476 Parent PID: 5328

General

Start time:	19:29:08
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe
Imagebase:	0x640000
File size:	564736 bytes
MD5 hash:	A665B705B9381B33AAA9E307FE340AF7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.571584010.0000000002981000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.571584010.0000000002981000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.568475564.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.568475564.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: BnevyAj.exe PID: 7036 Parent PID: 3352

General

Start time:	19:29:11
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Roaming\BnevyAj\BnevyAj.exe'
Imagebase:	0xf20000
File size:	564736 bytes
MD5 hash:	A665B705B9381B33AAA9E307FE340AF7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis