ID: 433461
Sample Name:
SecuriteInfo.com.Variant.Bulz.495766.21629.30464
Cookbook: default.jbs
Time: 22:38:25
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

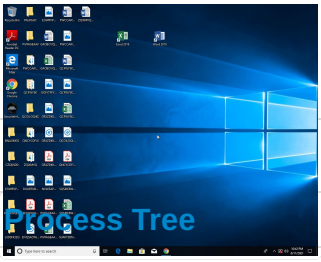
Analysis Report SecuriteInfo.com.Variant.Bulz.495766.2…

Overview

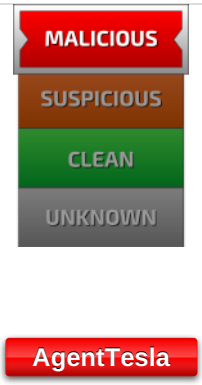
General Information

Sample Name:	SecuriteInfo.com.Variant.Bulz.495766.21629.30464 (renamed file extension from 30464 to exe)
Analysis ID:	433461
MD5:	755aff3a424238b..
SHA1:	d3c73271b37510..
SHA256:	41cba03f4c6ce7e..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

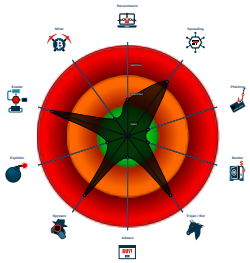


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: MSBuild connects …
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…

Classification



- **System is w10x64**
- SecuriteInfo.com.Variant.Bulz.495766.21629.exe (PID: 5760 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.495766.21629.exe' MD5: 755AFF3A424238B026F8D547783ECBD8)
  - MSBuild.exe (PID: 6036 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "Graceboy123@vivaldi.net",
  "Password": "4Lmm4pew4Z3EVCn",
  "Host": "smtp.vivaldi.net"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.211514974.000000000414 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.211514974.000000000414 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.211263032.000000000319 0000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000002.00000002.467134618.0000000002C5 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000002.00000000.208728671.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 7 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.0.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.0.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Variant.Bulz.495766.21629.exe.41f3898.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

Networking:

Sigma detected: MSBuild connects to smtp port

System Summary:

Sigma detected: Possible Applocker Bypass

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

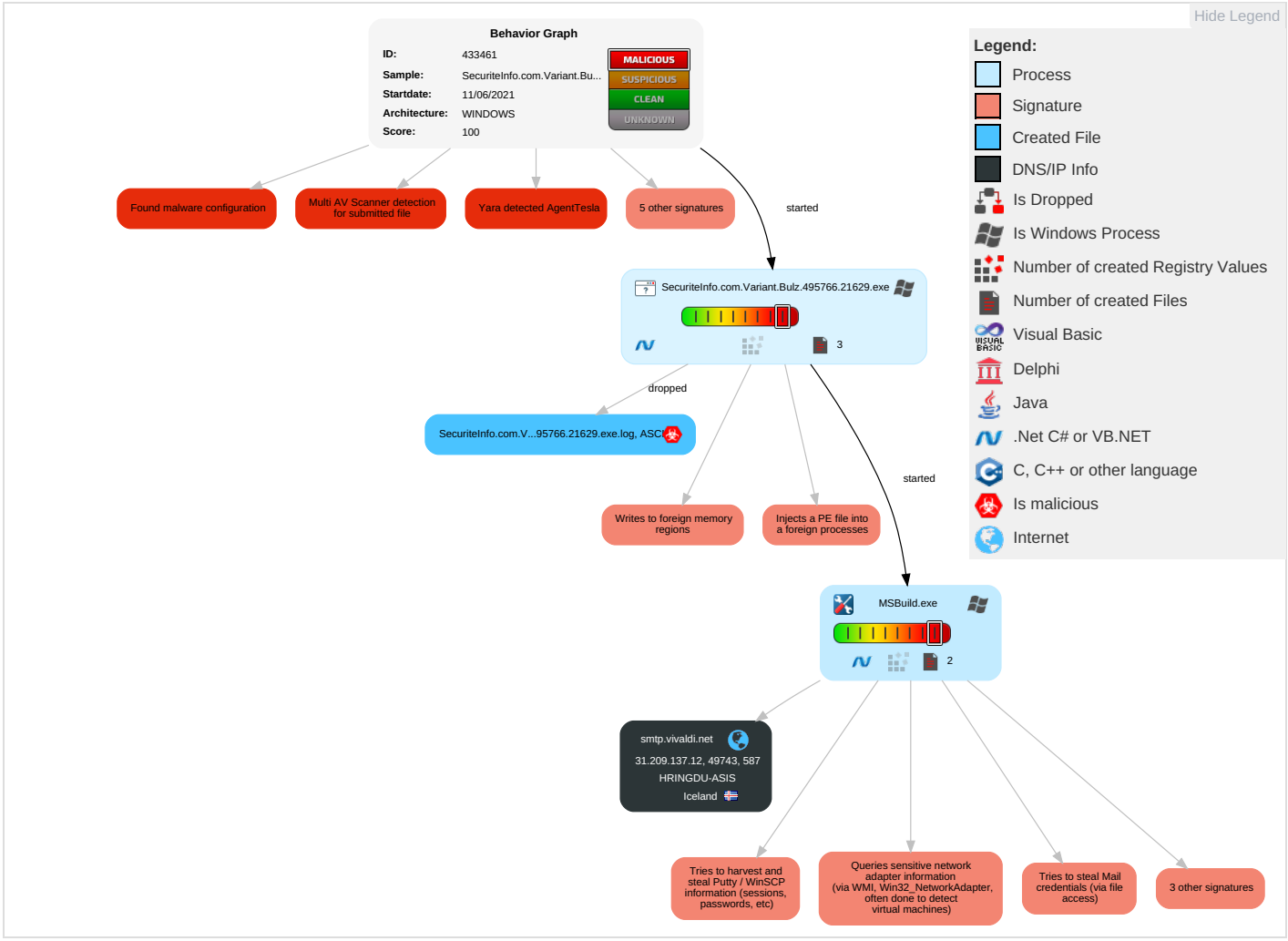
Yara detected AgentTesla

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	Path Interception	Process Injection 2 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 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	Process Discovery 2	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 2 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

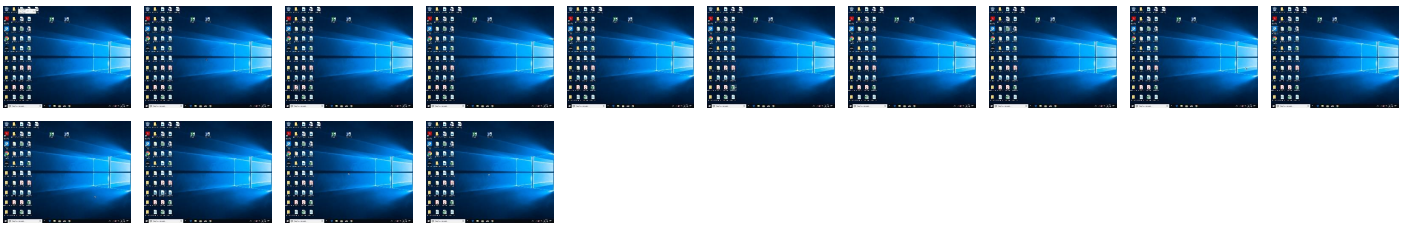
Behavior Graph



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

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Variant.Bulz.495766.21629.exe	38%	Virustotal		Browse
SecuriteInfo.com.Variant.Bulz.495766.21629.exe	30%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.MSBuild.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	

Source	Detection	Scanner	Label	Link
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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	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://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://api.ipify.org%h	0%	Avira URL Cloud	safe	
http://XkSLco.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.monotype.w	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://https://ntXEiMB2Wl.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	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://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.vivaldi.net	31.209.137.12	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.209.137.12	smtp.vivaldi.net	Iceland		51896	HRINGDU-ASIS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433461
Start date:	11.06.2021
Start time:	22:38:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Bulz.495766.21629.30464 (renamed file extension from 30464 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:	23
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.spre.troj.spyw.evad.winEXE@3/1@1/1
EGA Information:	Failed
HDC Information:	Failed
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
22:40:01	API Interceptor	45x Sleep call for process: SecuriteInfo.com.Variant.Bulz.495766.21629.exe modified
22:40:17	API Interceptor	788x Sleep call for process: MSBuild.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
31.209.137.12	COMMERCIAL INVOICE.exe	Get hash	malicious	Browse	
	Scan 07.07.2021# 99147.exe	Get hash	malicious	Browse	
	Quotes 04.06.2021.exe	Get hash	malicious	Browse	
	Quotes 07.06.2021.exe	Get hash	malicious	Browse	
	Proforma Invoice.pdf.exe	Get hash	malicious	Browse	
	PAYMENT FOR MS FOB 3-2027.exe	Get hash	malicious	Browse	
	Scan 03.06.2021.exe	Get hash	malicious	Browse	
	PAYMENT FOR MS FOB 3-2027.exe	Get hash	malicious	Browse	
	PAYMENT FOR MS FOB 3-2027.exe	Get hash	malicious	Browse	
	Scan 31.05.2021.exe	Get hash	malicious	Browse	
	PAYMENT FOR MS FOB 4-25.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	11,000euro.exe	Get hash	malicious	Browse	
	PURCHASE ORDER..exe	Get hash	malicious	Browse	
	PO2000254..exe	Get hash	malicious	Browse	
	BL Draft and Packing List.exe	Get hash	malicious	Browse	
	Purchase order.exe	Get hash	malicious	Browse	
	Y0wdyuqBy1mI2Y0.exe	Get hash	malicious	Browse	
	Items specifications.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	orders list.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.vivaldi.net	COMMERCIAL INVOICE.exe	Get hash	malicious	Browse	• 31.209.137.12
	Scan 07.07.2021# 99147.exe	Get hash	malicious	Browse	• 31.209.137.12
	Quotes 04.06.2021.exe	Get hash	malicious	Browse	• 31.209.137.12
	Quotes 07.06.2021.exe	Get hash	malicious	Browse	• 31.209.137.12
	Proforma Invoice.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	PAYMENT FOR MS FOB 3-2027.exe	Get hash	malicious	Browse	• 31.209.137.12
	Scan 03.06.2021.exe	Get hash	malicious	Browse	• 31.209.137.12
	PAYMENT FOR MS FOB 3-2027.exe	Get hash	malicious	Browse	• 31.209.137.12
	PAYMENT FOR MS FOB 3-2027.exe	Get hash	malicious	Browse	• 31.209.137.12
	Scan 31.05.2021.exe	Get hash	malicious	Browse	• 31.209.137.12
	PAYMENT FOR MS FOB 4-25.exe	Get hash	malicious	Browse	• 31.209.137.12
	11,000euro.exe	Get hash	malicious	Browse	• 31.209.137.12
	PURCHASE ORDER..exe	Get hash	malicious	Browse	• 31.209.137.12
	PO2000254..exe	Get hash	malicious	Browse	• 31.209.137.12
	BL Draft and Packing List.exe	Get hash	malicious	Browse	• 31.209.137.12
	Purchase order.exe	Get hash	malicious	Browse	• 31.209.137.12
	Y0wdyuqBy1mI2Y0.exe	Get hash	malicious	Browse	• 31.209.137.12
	Items specifications.exe	Get hash	malicious	Browse	• 31.209.137.12
	SOA.exe	Get hash	malicious	Browse	• 31.209.137.12
	orders list.exe	Get hash	malicious	Browse	• 31.209.137.12

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HRINGDU-ASIS	COMMERCIAL INVOICE.exe	Get hash	malicious	Browse	• 31.209.137.12
	Scan 07.07.2021# 99147.exe	Get hash	malicious	Browse	• 31.209.137.12
	Quotes 04.06.2021.exe	Get hash	malicious	Browse	• 31.209.137.12
	Quotes 07.06.2021.exe	Get hash	malicious	Browse	• 31.209.137.12
	Proforma Invoice.pdf.exe	Get hash	malicious	Browse	• 31.209.137.12
	PAYMENT FOR MS FOB 3-2027.exe	Get hash	malicious	Browse	• 31.209.137.12
	Scan 03.06.2021.exe	Get hash	malicious	Browse	• 31.209.137.12
	PAYMENT FOR MS FOB 3-2027.exe	Get hash	malicious	Browse	• 31.209.137.12
	PAYMENT FOR MS FOB 3-2027.exe	Get hash	malicious	Browse	• 31.209.137.12
	Scan 31.05.2021.exe	Get hash	malicious	Browse	• 31.209.137.12
	PAYMENT FOR MS FOB 4-25.exe	Get hash	malicious	Browse	• 31.209.137.12
	11,000euro.exe	Get hash	malicious	Browse	• 31.209.137.12
	PURCHASE ORDER..exe	Get hash	malicious	Browse	• 31.209.137.12
	PO2000254..exe	Get hash	malicious	Browse	• 31.209.137.12
	BL Draft and Packing List.exe	Get hash	malicious	Browse	• 31.209.137.12
	Purchase order.exe	Get hash	malicious	Browse	• 31.209.137.12
	Y0wdyuqBy1mI2Y0.exe	Get hash	malicious	Browse	• 31.209.137.12
	Items specifications.exe	Get hash	malicious	Browse	• 31.209.137.12
	SOA.exe	Get hash	malicious	Browse	• 31.209.137.12
	orders list.exe	Get hash	malicious	Browse	• 31.209.137.12

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Variant.Bulz.495766.21629.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.495766.21629.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1400
Entropy (8bit):	5.344635889251176
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEg:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHV
MD5:	394E646B019FF472CE37EE76A647A27F
SHA1:	BD5872D88EE9CD2299B5F0E462C53D9E7040D6DA
SHA-256:	2295A0B1F6ACD75FB5D038ADE65725EDF3DDF076107AEA93E4A864E35974AE2A
SHA-512:	7E95510C85262998AECC9A06A73A5BF6352304AF6EE143EC7E48A17473773F33A96A2F4146446444789B8BCC9B83372A227DC89C3D326A2E142BCA1E1A9B4809
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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.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\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.312014372881712
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.Variant.Bulz.495766.21629.exe
File size:	1559552
MD5:	755aff3a424238b026f8d547783ecbd8
SHA1:	d3c73271b3751043cdeb732e4c473fe462fbcd24
SHA256:	41cba03f4c6ce7e24b6f2d9f146a8cb82e9a43236859e82f14b225c2232adc5b
SHA512:	12b6e09d9c23b459e1d4ba9955a746be2e8ca6a9f905986522416551fd90e6b906126ffa1e3695ec525204e3e7dd8ae034acb01d7704b13f3c588783c9d79710
SSDEEP:	24576:OzSYNeBUdtwsEgwsHe/z8YEoqSg5LlJfH6zMIDsxTt8T2i9PGMbto2/siDUeuc/T:dYwBUwsEgwsHe5U/BldOSe+0eosic4YC
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...L..`.....P..D.....Rc... .....@.. .....@.....@.....

File Icon

Icon Hash:	e0c6a169f4bed870

Static PE Info

General

Entrypoint:	0x556352
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:	0x60C31E4C [Fri Jun 11 08:26:52 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
.text	0x2000	0x154358	0x154400	False	0.700508156916	data	7.40188775709	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x158000	0x28344	0x28400	False	0.599773146351	data	6.35187960045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x182000	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
Jun 11, 2021 22:40:57.994457006 CEST	192.168.2.3	8.8.8.8	0x45f6	Standard query (0)	smtp.vivaldi.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 22:40:58.056253910 CEST	8.8.8.8	192.168.2.3	0x45f6	No error (0)	smtp.vivaldi.net		31.209.137.12	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 11, 2021 22:40:58.887758017 CEST	587	49743	31.209.137.12	192.168.2.3	220 smtp.vivaldi.net ESMTP Postfix (Ubuntu)
Jun 11, 2021 22:40:58.888362885 CEST	49743	587	192.168.2.3	31.209.137.12	EHLO 045012
Jun 11, 2021 22:40:58.977018118 CEST	587	49743	31.209.137.12	192.168.2.3	250-smtp.vivaldi.net 250-PIPELINING 250-SIZE 36700160 250-ETRN 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 SMTPUTF8
Jun 11, 2021 22:40:58.977689981 CEST	49743	587	192.168.2.3	31.209.137.12	STARTTLS
Jun 11, 2021 22:40:59.066626072 CEST	587	49743	31.209.137.12	192.168.2.3	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Variant.Bulz.495766.21629.exe PID: 5760 Parent PID: 5880

General

Start time:	22:39:59
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.495766.21629.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Bulz.495766.21629.exe'
Imagebase:	0xc70000
File size:	1559552 bytes
MD5 hash:	755AFF3A424238B026F8D547783ECBD8
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: 00000000.00000002.211514974.0000000004141000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.211514974.0000000004141000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.211263032.0000000003190000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: MSBuild.exe PID: 6036 Parent PID: 5760

General

Start time:	22:40:06
Start date:	11/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0x770000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.467134618.0000000002C51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.208728671.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.208728671.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.463542809.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.463542809.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis