ID: 680333
Sample Name:
SecuriteInfo.com.Variant.Lazy.207585.14889.25639
Cookbook: default.jbs
Time: 12:06:12
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

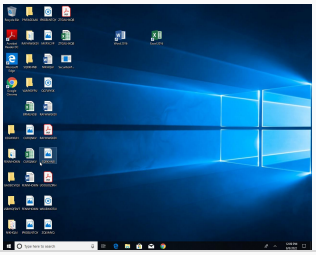
Windows Analysis Report

SecuriteInfo.com.Variant.Lazy.207585.14889.25639

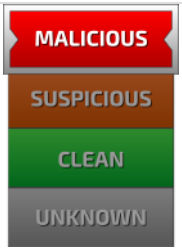
Overview

General Information

Sample Name:	SecuriteInfo.com.Variant.Lazy.207585.14889.25639 (renamed file extension from 25639 to exe)
Analysis ID:	680333
MD5:	62a5493cbeda91..
SHA1:	9e6941500fbb55..
SHA256:	60383046971044.
Tags:	exe
Infos:	



Detection



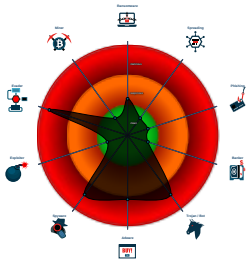
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Variant.Lazy.207585.14889.exe (PID: 1100 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Variant.Lazy.207585.14889.exe" MD5: 62A5493CBEDA91C0D3B7593BB0A00424)
  - RegSvcs.exe (PID: 5980 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 3736 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "ventas@bluemix.cl",
  "Password": "bluemix2020737",
  "Host": "mail.bluemix.cl"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.268432848.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000000.268432848.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000000.268432848.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x301f8:$a13: get_DnsResolver • 0x2ea06:$a20: get_LastAccessed • 0x30b76:$a27: set_InternalServerPort • 0x30e95:$a30: set_GuidMasterKey • 0x2eb0d:$a33: get_Clipboard • 0x2eb1b:$a34: get_Keyboard • 0x2fe13:$a35: get_ShiftKeyDown • 0x2fe24:$a36: get_AltKeyDown • 0x2eb28:$a37: get_Password • 0x2f5c3:$a38: get_PasswordHash • 0x305f8:$a39: get_DefaultCredentials
00000000.00000002.280169100.0000000003699000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.280169100.0000000003699000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
6.0.RegSvcs.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32cc1:$s10: logins • 0x32728:$s11: credential • 0x2ed0d:$g1: get_Clipboard • 0x2ed1b:$g2: get_Keyboard • 0x2ed28:$g3: get_Password • 0x30003:$g4: get_CtrlKeyDown • 0x30013:$g5: get_ShiftKeyDown • 0x30024:$g6: get_AltKeyDown
6.0.RegSvcs.exe.400000.0.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x303f8:$a13: get_DnsResolver • 0x2ec06:$a20: get_LastAccessed • 0x30d76:$a27: set_InternalServerPort • 0x31095:$a30: set_GuidMasterKey • 0x2ed0d:$a33: get_Clipboard • 0x2ed1b:$a34: get_Keyboard • 0x30013:$a35: get_ShiftKeyDown • 0x30024:$a36: get_AltKeyDown • 0x2ed28:$a37: get_Password • 0x2f7c3:$a38: get_PasswordHash • 0x307f8:$a39: get_DefaultCredentials
0.2.SecuriteInfo.com.Variant.Lazy.207585.14889.exe.384c890.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 11 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

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

Writes to foreign memory regions

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the hosts file

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality

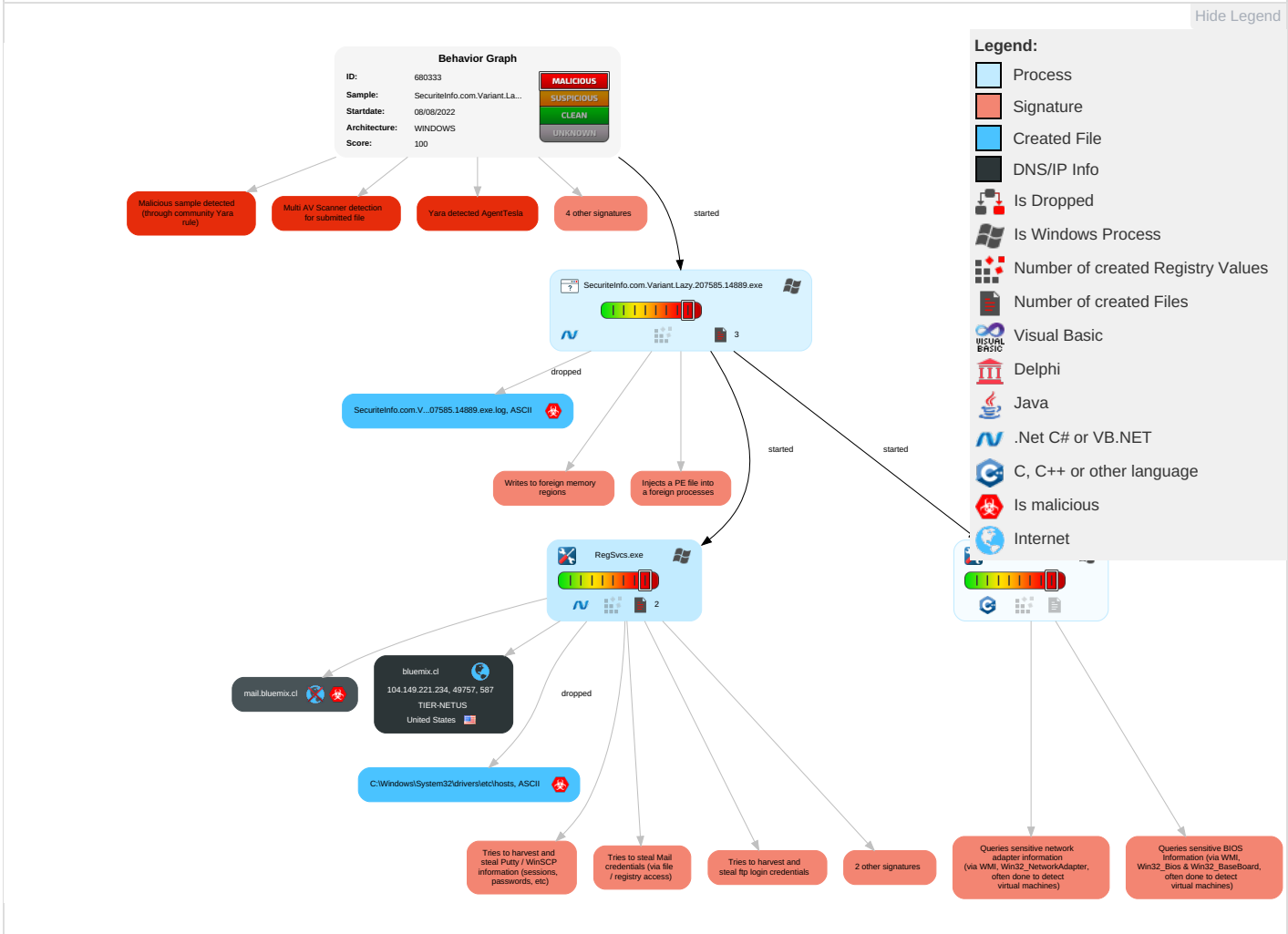
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	2 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 File and Directory Permissions Modification	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 3 1 Virtualization/Sandbox Evasion	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 1 1 Process Injection	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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.Lazy.207585.14889.exe	58%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Variant.Lazy.207585.14889.exe	36%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
SecuriteInfo.com.Variant.Lazy.207585.14889.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
bluemix.cl	0%	Virustotal		Browse
mail.bluemix.cl	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fonts.comig4	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.fonts.comP	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://d1GB0YAapow6XmOM.org	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://mail.bluemix.cl	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://BhHVua.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://bluemix.cl	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.fonts.combig	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

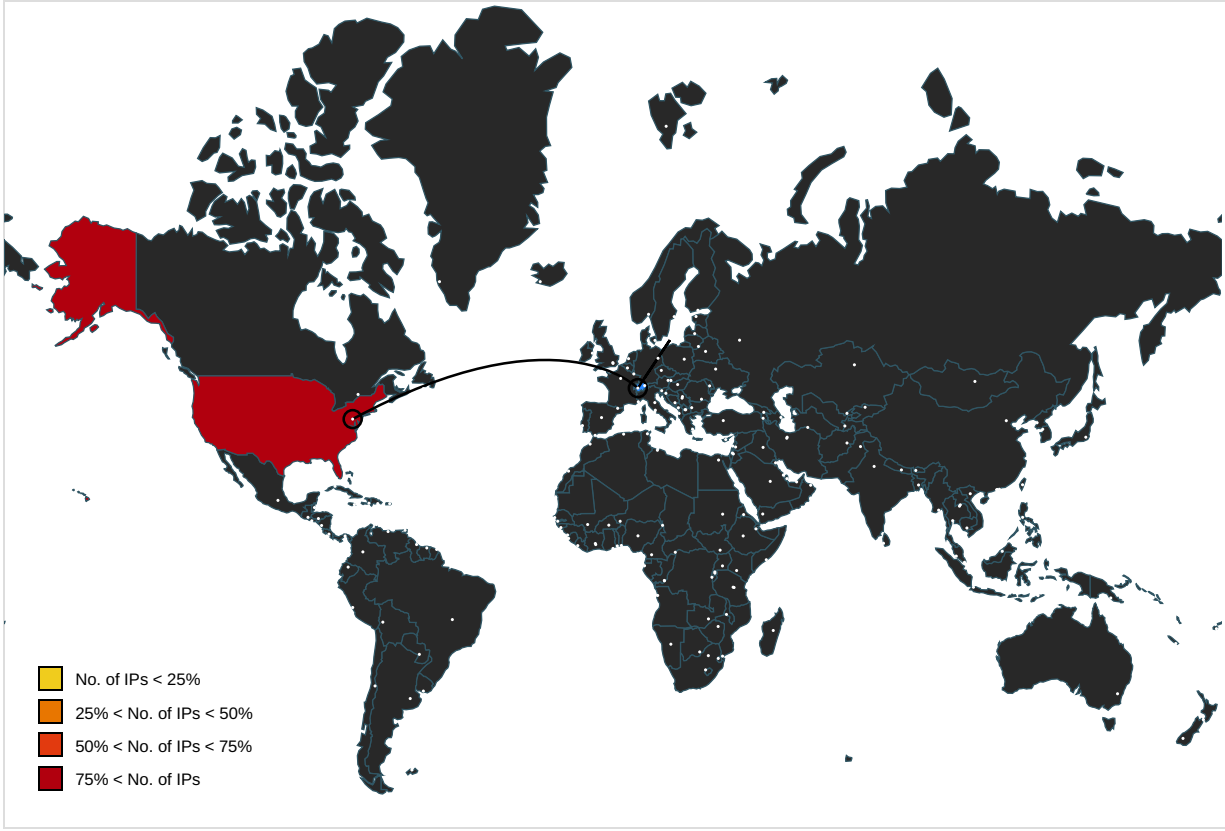
Name	IP	Active	Malicious	Antivirus Detection	Reputation
bluemix.cl	104.149.221.234	true	false	• 0%, Virustotal, Browse	unknown
mail.bluemix.cl	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 00000006.00000002.501747915.0000000002A31000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0	RegSvcs.exe, 00000006.00000002.508271478.0000000005D98000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000006.00000002.505019128.0000000002D8E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.comig4	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000003.235850074.0000000000CEC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	RegSvcs.exe, 00000006.00000002.501747915.0000000002A31000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comP	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000003.235850074.0000000000CEC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%%startupfolder%	RegSvcs.exe, 00000006.00000002.501747915.0000000002A31000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.goodfont.co.kr	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://d1GB0YAapow6XmOM.org	RegSvcs.exe, 00000006.00000002.501747915.0000000002A31000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000006.00000002.505118218.0000000002DB2000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000006.00000002.505142726.0000000002DBA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false		high
http://mail.bluemix.cl	RegSvcs.exe, 00000006.00000002.505019128.0000000002D8E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	RegSvcs.exe, 00000006.00000002.501747915.0000000002A31000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://BhHVua.com	RegSvcs.exe, 00000006.00000002.501747915.0000000002A31000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000003.235850074.0000000000CEC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://bluemix.cl	RegSvcs.exe, 00000006.00000002.505019128.0000000002D8E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.combig	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000003.235850074.0000000000CEC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	SecuriteInfo.com.Variant.Lazy.207585.14889.exe, 00000000.00000002.285875757.0000000006812000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	RegSvcs.exe, 00000006.00000002.501747915.0000000002A31000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.149.221.234	bluemix.cl	United States		397423	TIER-NETUS	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680333
Start date and time: 08/08/202212:06:12	2022-08-08 12:06:12 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Lazy.207585.14889.25639 (renamed file extension from 25639 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:	28
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.adwa.spyw.evad.winEXE@5/2@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 88% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:07:27	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Variant.Lazy.207585.14889.exe modified
12:07:35	API Interceptor	699x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

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.Lazy.207585.14889.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Lazy.207585.14889.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3

SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
Reputation:	high, 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..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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA F
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.41549459780222
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SecuriteInfo.com.Variant.Lazy.207585.14889.exe
File size:	884736
MD5:	62a5493cbeda91c0d3b7593bb0a00424
SHA1:	9e6941500fbb55c643ce5e59e3bd86e114f4a73d
SHA256:	60383046971044bc8d25ec8a3cc0bf559dca620af2b978d2cd7f5c35363c44c5
SHA512:	28c2432e27bc3964a61c27dc5ba1ef98dea9f8a7f07e6bed32dfd42d18399f18c3cc952a394d15c494d0b4195552ef5f0f8925998e671810cc98f27909159e69
SSDEEP:	12288:mhBQEIjT6JFjwi9BZNbvYbagLEtxGmfVMmI/OLB8DIEBIvfkOJxjza39AeLKvrBl:quzkjwi9BHtgL4p8OLmBIjzjZ
TLSH:	0E155CA8319072DED927CA31CAA41C74EA617C77A71B921794633299DF3E987DF100B3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....U.b.....P..j..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d892e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F055E1 [Mon Aug 8 00:16:33 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd88d4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xda000	0x11f0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xdc000	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	0xd6934	0xd6a00	False	0.7423740535818287	data	7.41882242323763	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xda000	0x11f0	0x1200	False	0.3927951388888889	data	5.044747416478067	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xdc000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xda0a0	0x334	data		
RT_MANIFEST	0xda3d4	0xe15	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

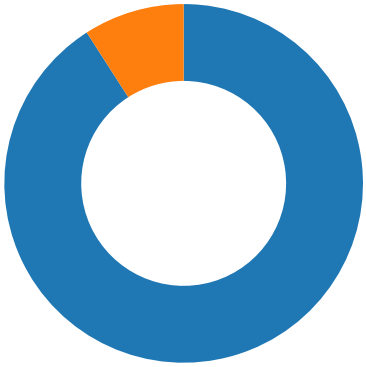
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution

Total Packets: 22

- 53 (DNS)
- 587 undefined



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:07:50.903929949 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:51.060014963 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:51.060251951 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:51.277803898 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:51.278224945 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:51.434055090 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:51.434320927 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:51.592422962 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:51.629565954 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:51.797372103 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:51.797389030 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:51.797400951 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:51.797409058 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:51.797485113 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:51.797517061 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:51.801029921 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:51.830961943 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:51.986874104 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:52.049287081 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:52.133793116 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:52.290673018 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:52.292047977 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:52.449750900 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:52.450333118 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:52.630346060 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:52.631134033 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:52.787030935 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:52.787491083 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:52.951402903 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:52.951924086 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:53.107825041 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:53.108823061 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:53.108947039 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:53.109611988 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:53.109689951 CEST	49757	587	192.168.2.4	104.149.221.234
Aug 8, 2022 12:07:53.264444113 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:53.264504910 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:53.265361071 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:53.265377998 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:53.448128939 CEST	587	49757	104.149.221.234	192.168.2.4
Aug 8, 2022 12:07:53.643105030 CEST	49757	587	192.168.2.4	104.149.221.234

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:07:50.034467936 CEST	62099	53	192.168.2.4	8.8.8.8
Aug 8, 2022 12:07:50.425446033 CEST	53	62099	8.8.8.8	192.168.2.4
Aug 8, 2022 12:07:50.483175993 CEST	53775	53	192.168.2.4	8.8.8.8
Aug 8, 2022 12:07:50.875464916 CEST	53	53775	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 12:07:50.034467936 CEST	192.168.2.4	8.8.8.8	0xe61e	Standard query (0)	mail.bluemix.cl	A (IP address)	IN (0x0001)
Aug 8, 2022 12:07:50.483175993 CEST	192.168.2.4	8.8.8.8	0x5ca5	Standard query (0)	mail.bluemix.cl	A (IP address)	IN (0x0001)

DNS Answers

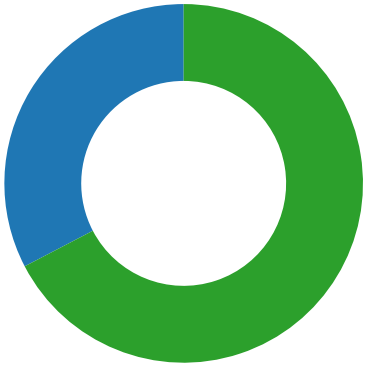
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 12:07:50.425446033 CEST	8.8.8.8	192.168.2.4	0xe61e	No error (0)	mail.bluemix.cl	bluemix.cl		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 12:07:50.425446033 CEST	8.8.8.8	192.168.2.4	0xe61e	No error (0)	bluemix.cl		104.149.221.234	A (IP address)	IN (0x0001)
Aug 8, 2022 12:07:50.875464916 CEST	8.8.8.8	192.168.2.4	0x5ca5	No error (0)	mail.bluemix.cl	bluemix.cl		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 12:07:50.875464916 CEST	8.8.8.8	192.168.2.4	0x5ca5	No error (0)	bluemix.cl		104.149.221.234	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 8, 2022 12:07:51.277803898 CEST	587	49757	104.149.221.234	192.168.2.4	220-srv34.benzahosting.cl ESMTP Exam 4.95 #2 Mon, 08 Aug 2022 06:07:51 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 8, 2022 12:07:51.278224945 CEST	49757	587	192.168.2.4	104.149.221.234	EHLO 067773
Aug 8, 2022 12:07:51.434055090 CEST	587	49757	104.149.221.234	192.168.2.4	250-srv34.benzahosting.cl Hello 067773 [102.129.143.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 8, 2022 12:07:51.434320927 CEST	49757	587	192.168.2.4	104.149.221.234	STARTTLS
Aug 8, 2022 12:07:51.592422962 CEST	587	49757	104.149.221.234	192.168.2.4	220 TLS go ahead

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Variant.Lazy.207585.14889.exe PID: **1100**, Parent PID: **5016**

General

Target ID:	0
Start time:	12:07:14
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Lazy.207585.14889.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Variant.Lazy.207585.14889.exe"
Imagebase:	0x1d0000
File size:	884736 bytes
MD5 hash:	62A5493CBEDA91C0D3B7593BB0A00424
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: 00000000.00000002.280169100.0000000003699000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.280169100.0000000003699000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.280169100.0000000003699000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.275554875.00000000028E4000.00000004.00000800.00020000.00000000.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	6CD1CF06	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	6CD1CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Variant.Lazy.207585.14889.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D02C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Variant.Lazy.207585.14889.exe.log	0	1216	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 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 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 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	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D02C907	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	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BB61B4F	ReadFile

Analysis Process: RegSvcs.exe PID: **5980**, Parent PID: **1100**

General

Target ID:	4
Start time:	12:07:30
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0xb0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: RegSvcs.exe PID: **3736**, Parent PID: **1100**

General

Target ID:	6
Start time:	12:07:31
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x5f0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000006.00000000.268432848.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.268432848.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000006.00000000.268432848.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.501747915.0000000002A31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.501747915.0000000002A31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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	6CD1CF06	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	6CD1CF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	6BB61B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6CCFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CCFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CC503DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BB61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BB61B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\d1aef8e4-b864-479c-bf86-f42c63d352b2	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BB61B4F	ReadFile

Disassembly

No disassembly