ID: 528564
Sample Name:
SecuriteInfo.com.MachineLearning.Anomalous.94.14541.14773
Cookbook: default.jbs
Time: 14:04:37
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

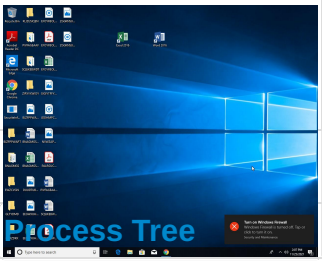
Windows Analysis Report SecuriteInfo.com.MachineLea…

Overview

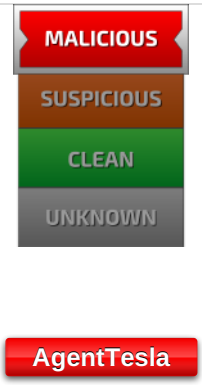
General Information

Sample Name:	SecuriteInfo.com.MachineLearning.Anomalous.94.14541.14773 (renamed file extension from 14773 to exe)
Analysis ID:	528564
MD5:	4ce54eda7650ff0..
SHA1:	0eaa03d538e574..
SHA256:	9246176ddd535c..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

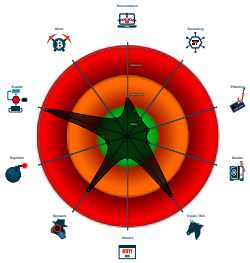


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fil…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Queries sensitive video device inform…
- Sigma detected: Powershell Defende…
- .NET source code contains very larg…
- Adds a directory exclusion to Windo…
- Queries sensitive network adapter in…

Classification



- **System is w10x64**
- SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe (PID: 6176 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe" MD5: 4CE54EDA7650FF0F8062189F089B162E)
  - powershell.exe (PID: 7052 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe (PID: 4396 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe MD5: 4CE54EDA7650FF0F8062189F089B162E)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "m@huiijingco.com",
  "Password": "lNLUrZT2",
  "Host": "smtp.huiijingco.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.302889154.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.302889154.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000002.561614573.0000000002AA6000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000000.302163969.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.302163969.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe.3730f20.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe.3730f20.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.0.SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe.400000.10.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.0.SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 17 entries				

Sigma Overview

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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:

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

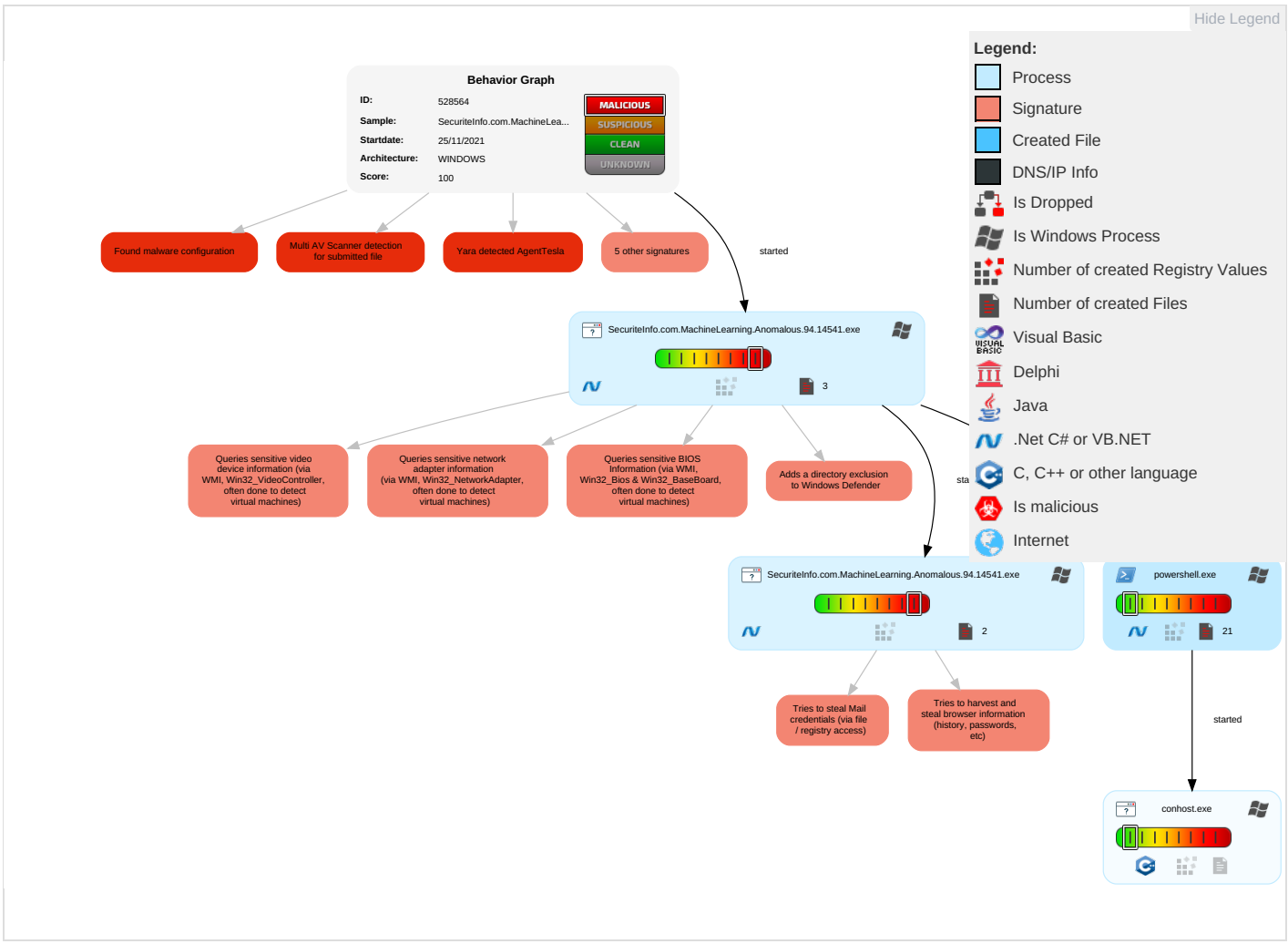
Remote Access Functionality:

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 3 1 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 3 2 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 4 1	Security Account Manager	Virtualization/Sandbox Evasion 2 4 1	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Account 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	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

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.MachineLearning.Anomalous.94.14541.exe	15%	Virustotal		Browse
SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe	16%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe.400000.4.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://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://XYJLds.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://api.ipify.org%	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	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528564
Start date:	25.11.2021
Start time:	14:04:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.MachineLearning.Anomalous.94.14541.14773 (renamed file extension from 14773 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:	20
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@6/4@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • 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
14:05:36	API Interceptor	758x Sleep call for process: SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe modified
14:05:40	API Interceptor	42x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22284
Entropy (8bit):	5.601591505646068
Encrypted:	false
SSDEEP:	384:1tCD2q0LOkO1R8MYB9PRwS0nUjultI2H7Y9gtrSJ3xCT1MabZlbAV7lW2LWZBDIr:q1R8MYBETUCltJXxcQCqfw8VQ
MD5:	4D124085F73CFF9200F6CDFCFB6EC839
SHA1:	98910C984B94FB2247EED9AAD4536467C513A785
SHA-256:	1245D0CAEA84E856F84675B49D143C7C5C645DD737A64E6158FF22A2204F05AD
SHA-512:	4410C52F276599D933F5D43A7B6EB2A00383B8715C0F8C37CDCBAFB52D3AA1EA9BDCC50A5DB48689067049BD4FA0D77EF83FFF54B91F5AE86BE6F1268F1F89 5
Malicious:	false
Reputation:	low
Preview:	@...e.....|.....h...[.Q.N.....F.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_b1j2o2gx.24c.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_f0qsiy5n.jol.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\Documents\20211125\PowerShell_transcript.287400.d+yQR6Ej.20211125140539.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5921
Entropy (8bit):	5.380444983318727
Encrypted:	false
SSDEEP:	96:BZUh5N/tqDo1Z7Zjh5N/tqDo1ZRga4jZ7h5N/tqDo1Zi9oodZa:1
MD5:	4A1BB70E8685422D7051C4D6C5CC2F40
SHA1:	D995EC8EEFDA7F5959E7821D4A22F53336B3978C
SHA-256:	742AA9A762245844C70FD0C35A6872E9E500520F1CBA9A5351BC3DB7BC6F5D6E
SHA-512:	2C89B4B8A15F37FDF73FFBD3847DFA68F88165447479458256BBE7F3AE530336899EED0060D04AFB336A0C9CAB4D18BD163DBDBD7AF4D6293312C2D326158E9E
Malicious:	false
Reputation:	low
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211125140540..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 287400 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe..Process ID: 7052..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211125140540..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe..**********..Windows PowerShell transcript start..Start time: 20211125140932.

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.868157297120685

General

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.MachineLearning.Anomalous.94.14541.exe
File size:	498688
MD5:	4ce54eda7650ff0f8062189f089b162e
SHA1:	0eaa03d538e574a17ac685b3356816f696e47f4b
SHA256:	9246176ddd535c1d48514759ef33e8a129dc6881f685580484a8291940ea5e85
SHA512:	2a04edb11d4d26580cc3d39840897b273b0c33fdae8a0a8f4649ce5318a9cabfd8e30961dc625cb6d1720611bf7098b7d19ef0fefc93615dd0c0105436be6d59
SSDEEP:	12288:f8sBOM0eixBFmzbSyuEpAgXoXJTo2+9A3x2pHlAQomss61Qna:f8sAM0ei1EcEr8Smh2pHlAL+61Qna
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Y.a.....0..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47b0b6
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:	0x619F59DB [Thu Nov 25 09:39:39 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	0x790cc	0x79200	False	0.895851473813	data	7.8787752496	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7c000	0x5ec	0x600	False	0.438802083333	data	4.2127347954	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7e000	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

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe PID: 6176 Parent PID: 6076

General

Start time:	14:05:35
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe"
Imagebase:	0xa0000
File size:	498688 bytes
MD5 hash:	4CE54EDA7650FF0F8062189F089B162E
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: 00000000.00000002.307311514.000000000360D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.307311514.000000000360D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.306897551.00000000026CB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.306734942.0000000002601000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: powershell.exe PID: 7052 Parent PID: 6176

General

Start time:	14:05:38
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe
Imagebase:	0xaa0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6120 Parent PID: 7052

General

Start time:	14:05:38
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe PID: 4396 Parent PID: 6176

General

Start time:	14:05:39
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.MachineLearning.Anomalous.94.14541.exe
Imagebase:	0x5a0000
File size:	498688 bytes

MD5 hash:	4CE54EDA7650FF0F8062189F089B162E
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: 00000003.00000000.302889154.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.302889154.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.561614573.0000000002AA6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.302163969.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.302163969.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.303645199.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.303645199.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.558585999.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.558585999.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.304322848.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.304322848.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.561540935.00000000029F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.561540935.00000000029F1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis